Inhoudsopgave

Sinds januari 2016 is het verplicht datalekken te melden als dit nadelige gevolgen kan hebben voor patiënten, zoals een lek met medische gegevens. De Handreiking Meldplicht Datalekken helpt apothekers bij het omgaan met een datalek.

De Algemene Verordening Gegevensbescherming (AVG) verplicht alle datalekken te documenteren, ook wanneer er geen meldingsplicht is aan de Autoriteit Persoonsgegevens (AP) en/of de patiënt. Het doel van documenteren is om in de toekomst zo veel mogelijk datalekken te voorkomen. Een ander doel is om de AP aan te tonen dat datalekken daadwerkelijk worden gemonitord en opgevolgd.

Het documenteren van een datalek kan vaak in een bestaand kwaliteits- of incidentmeldsysteem. Indien deze niet beschikbaar zijn, kunnen apothekers dit register gebruiken.

Het register datalekken is opgemaakt met voorgedefinieerde teksten om eenvoudig een datalek te documenteren. Voor een aantal kolommen kan een keuze gemaakt worden uit voorgedefinieerde teksten. Deze kunnen naderhand bijgewerkt of aangevuld worden. Daarnaast staan de kolommen in chronologische volgorde.

Toelichting kolommen

Datum	TopDesk	Inbreuk: gegevens zijn (onbevoegd)	Beschrijving van de inbreuk	(Mogelijke) gevolgen Getroffen maatregelen	Melding aan AP?	Datum melding	Melding betrokkene(n)	Datum melding	Tekst kennisgeving aan betrokkene(n)	Verantw	Afdeling team	Categorie
01-10-2015		Gelezen (vertrouwelijkheid)	Medewerker GT heeft informatie gebruikt die hij niet had mogen gebruiken		Nee, voorlopig ingetrokken		Nee			Dan-Coll	M&S / GT	Overig
14-03-2019	C1903 3144	Gelezen (vertrouwelijkheid)	Bij de printer lag een gewaarmerkt afschrift uit BRP	Mdw's BuZa gevraagd deze printer uit printlijst te verwijderen. Printer is verwijderd uit BRP-systeem	Nee		Nee			Dan-Coll	KCC / Boargersaken	Persoonsgegevens per ongeluk gepubliceerd
03-04-2019	C1904 707	Gelezen (vertrouwelijkheid)	In 138 brieven met een verzoek om bankgegevens in te leveren ivm kwijtschelding is een verkeerd bankrekeningnummer geprint	Misbruik van bankrekeningnummers (niet herleidbaar naar rekeninghouders). Herstelbrieven verstuurd.	Nee					Dan-Coll		Persoonsgegevens per ongeluk gepubliceerd
18-04-2019	C1904 4197	Gelezen (vertrouwelijkheid)	Voor urgentieverklaring WMO ThusWonen heeft medewerker naam van de melder aan TW gegeven		Nee		Ja		Melder geadviseerd om te melden aan betrokkene	Dan-Coll	M&S / WMO	Persoonsgegevens per ongeluk gepubliceerd
12-07-2020	C2007-2901	Gelezen (vertrouwelijkheid)	In een bijlage op RIS zijn persoonsgegevens onvoldoende onleesbaar gemaakt waardoor deze via een omweg toch getoond konden worden	Bestand is verwijderd en wordt vervangen door correct geanonimiseerd bestand	Nee		Nee			Dan-Coll		Persoonsgegevens per ongeluk gepubliceerd
15-10-2020	C2010-3604	Gelezen (vertrouwelijkheid)	Een CSV-bestand met BSN+NAW van 170 personen uit BRP-productie is gebruikt voor testen MyLex en onvoldoende beveiligd naar leverancier verstuurd	Bestand vernietigd door ontvangen.	Nee	17-10-2020	Nee			Dan-Coll		Overig
25-05-2021	C2105-4687	Geen / overig	Mail verzonden naar verkeerde ontvanger. Mail bevatte geen persoonsgegevens.	Geen datalek in de zin van de AVG.	Nee		Nee			Dan-Coll	M&S / Jeugd	Persoonsgegevens aan verkeerde ontvanger(s) verstuurd
08-06-2021	C2106-1939	Geen / overig	Intern bedoelde mail verstuurd naar extern adres	Mail is niet verzonden, kon door SSC worden tegengehouden	Nee		Nee			Dan-Coll	Griffy-Dan	Persoonsgegevens aan verkeerde ontvanger(s) verstuurd
20-10-2021	C2110-4833	Gelezen (vertrouwelijkheid)	Gedurende een half uur heeft een document met gegevens online gestaan op RIS	Omdat document van iBabs is verwijderd kan niet meer nagegaan worden of en door wie (IP) het document is gezien	Nee		Nee			Dan-Raad	Griffy-Dan	Persoonsgegevens per ongeluk gepubliceerd
21-10-2021	C2110-5109	Gelezen (vertrouwelijkheid)	Ongeanomimiseerde documenten met gegevens van ruim 70 personen verstuurd. Betreft bezwaren en zienswijzen	Ontvangers verzocht documenten te wissen of vernietigen	Nee		Nee			Dan-Coll	BF / JS	Persoonsgegevens per ongeluk gepubliceerd
01-11-2021	C2111-0231	Gelezen (vertrouwelijkheid)	AD-inloggegevens (gebruikersnaam en wachtwoord) wegens ziekte gedeeld met collega	Account geblokkeerd.	Nee		Nee			Anders	M&S / WMO	Overig
03-01-2022	C2201-0346	Gekopieerd	Brief inwoner doorgestuurd aan ondernemer (BING-onderzoek DA)	Verzocht om document/mail te wissen	Nee		Nee			Dan-Coll		Overig
22-02-2022	C2202-5770	Gelezen (vertrouwelijkheid)	Een raadsfractie heeft vragen gesteld, hierbij is een adressenlijst met 88 voornamelijk particuliere woonadressen geleverd en gepubliceerd op de raadswebsite.	Lijst is van de raadswebsite verwijderd.	Nee		Nee			Dan-Coll	Griffy-Dan	Persoonsgegevens per ongeluk gepubliceerd
20-09-2022	C2209-4751	Gelezen (vertrouwelijkheid)	Vanuit DJI (Justitie) terugkeeradres ontvangen van cliënt. Hier hebben wij een ondersteuningsbrief naar verzonden. In de brief is per ongeluk de aanhef van vader van cliënt gebruikt. Cliënt blijkt ook niet op dit adres te verblijven, onbekend is waar wel. De informatie in de brief betreft einde detentie en het aanbod tot ondersteuning vanuit Gemeente. Vader heeft ons gebeld, waarna de datalek is geconstateerd.		Ja		Nee		Wegens adres onbekend geen k	Dan-Coll	M&S / GT	Persoonsgegevens aan verkeerde ontvanger(s) verstuurd
08-12-2022	C2212-2384	Gelezen (vertrouwelijkheid)	Datalek BZF-Leeuwarden: drie ondernemers hebben gegevens ontvangen van 8800 TOZO-gebruikers, waaronder ook gegevens uit NF en DA.	Ontvangers hebben aangegeven bestand te hebben verwijderd			Ja		Zie brief gemeente Leeuwarden		Extern	Persoonsgegevens per ongeluk gepubliceerd
13-02-2023	C2302-3217	Geen / overig	Raadslid is toegangsbadge kwijt.	Badge is geblokkeerd. Inmiddels teruggevonden en ingeleverd.	Nee		Nee			Dan-Raad		Overig
27-03-2023	C2303-6778	Gelezen (vertrouwelijkheid)	Bij kopiëren in Excel is een mailadres verwisseld. Hierdoor heeft een inwoner informatie (witgoedwissel) gekregen over een andere persoon	Telefonisch contact gehad met ontvanger. Betrof alleen een naam van de betrokkene.	Nee		Nee			Dan-Coll	M&S	Persoonsgegevens aan verkeerde ontvanger(s) verstuurd
13-07-2023	C2307-3236	Gelezen (vertrouwelijkheid)	Op 4 juli 2023 heeft een inwoner per mail een brief aan het college Dantumadiel gestuurd over de publicatie van haar persoonsgegevens in een zienswijze tegen een bestemmingsplan (zie REX 2023-159065).							Dan-Coll		Persoonsgegevens per ongeluk gepubliceerd
06-11-2023	C2311-1327	Gelezen (vertrouwelijkheid)	Bij verzenden van een mail aan ongeveer 30 inwoners zijn de ontvangers niet in bcc gezet.	Ontvangers zijn verzocht de mail te verwijderen. Voor zover bekend twee bevestigingen van verwijdering ontvangen.	Nee		Nee					Persoonsgegevens per ongeluk gepubliceerd

Datum	TopDesk	Inbreuk: gegevens zijn (onbevoegd)	Beschrijving van de inbreuk	(Mogelijke) gevolgen Getroffen maatregelen	Melding aan AP?	Datum melding	Melding betrokkene(n)	Datum melding	Tekst kennisgeving aan betrokkene(n)	Verantw	Afdeling team	Categorie
20-12-2023	C2312-5190	Geen / overig	Bij uitreiken van inloggegevens aan medewerkers Dantumadiel bleken twee enveloppen met de inloggegevens te ontbreken	Bij de ontvangst van de enveloppen is niet geteld of alle enveloppen aanwezig waren. Het document bevat een inlognaam en en password dat bij de eerste inlog gewijzigd moet worden. Uit controle blijkt dat de twee ontbrekende gegevens niet zijn gebruikt	Nee		Nee					Overig
21-12-2023	C2312-5428	Gelezen (vertrouwelijkheid)	Op de raadswebsite is een document met persoonsgegevens gepubliceerd	Document is achter slotje geplaatst.	Nee		Nee					Persoonsgegevens per ongeluk gepubliceerd

Afdeling/team	Inbreuk	Melding aan AP?
Bedriuwsfiering	Ontvreemd	Ja
Bestuurssecretariaat	Gekopieerd	Ja, voorlopig
BF / Adm Belestingen	Gelezen (vertrouwelijkheid)	Nee
BF / P&O	Veranderd (integriteit)	Nee, voorlopig ingetrokken
BF/Feiligens	Verwijderd of vernietigd (beschikbaar)	
DW	Nog niet bekend	
DW / Iepenbiere Rom	Geen / overig	
Griffy-Dan		
Griffy-NF		
GW		
KCC / Boargersaken		
KCC / Fergunnings		
KKS		
M&S		
M&S / Adm		
M&S / Belied		
M&S / GT		
M&S / Jeugd		
M&S / SHV		
M&S / WMO		
M&S / Ynk		
NEF		
BF / G&A		
Directie		
FTH / Fergunning		
BF / Fin Belied		
BF / Fin Beheer		
Yngenieursbureau		
BF / JS		
Extern		
Mienskip		

Melden betrokkene(n)	Verantwoordelijke	Gegevens zijn
Ja, datalek vormt waarschijnlijk een (hoog) risico	Dan-Bm	
Nee, getroffen maatregelen bieden voldoende bescherming	Dan-Coll	
Nee, gevolgen onwaarschijnlijk	Dan-Raad	
Nee, zwaarwegende redenen	NF-BM	
	NF-Coll	
	NF-Raad	
	Schiermonnikoog	
	Anders	

Aantal betrokkenen	Gevolgen	Categorie
Enkel (1)		E-mail aan verkeerde ontvanger(s)
Aantal (<10)		E-mail met ontvangers niet in de bcc
Tientallen (<100)		Brief verstuurd aan de verkeerde ontvanger(s)
Honderden (<1.000)		Brief geopend retour ontvangen
Duizenden (<10.000)		Brief of postpakket kwijtgeraakt
Allen		Autorisatie(s) verkeerd ingesteld
		Netwerkmappen te breed toegankelijk
		Apparaat of doc's kwijtgeraakt of gestolen
		Pgg per ongeluk gepubliceerd
		Phishing
		Ransomware
		Ander type hacking en/of malware
		Raadplegen van pgg zonder legitiem doel
		Pgg van verkeerde klant getoond in portaal
		Pgg toegevoegd aan het verkeerde dossier
		Pgg bij oud papier gezet
		Pgg door storing (tijdelijk) niet beschikbaar
		Overig

Categorie	2017	2018	2019	2021	2022	2023	2024
E-mail aan verkeerde ontvanger(s)	-	-	-	-	-	11	6
E-mail met ontvangers niet in de bcc	-	-	-	-	-	-	-
Brief verstuurd aan de verkeerde ontvanger(s)	-	-	-	-	-	-	2
Brief geopend retour ontvangen	-	-	-	-	-	-	-
Brief of postpakket kwijtgeraakt	-	-	-	-	-	-	-
Autorisatie(s) verkeerd ingesteld	-	-	-	-	-	-	1
Netwerkmappen te breed toegankelijk	-	-	-	-	-	-	-
Apparaat of doc's kwijtgeraakt of gestolen	-	-	-	-	-	1	1
Pgg per ongeluk gepubliceerd	-	-	-	-	-	18	1
Phishing	-	-	-	-	-	-	-
Ransomware	-	-	-	-	-	-	-
Ander type hacking en/of malware	-	-	-	-	-	-	-
Raadplegen van pgg zonder legitiem doel	-	-	-	-	-	-	-
Pgg van verkeerde klant getoond in portaal	-	-	-	-	-	1	-
Pgg toegevoegd aan het verkeerde dossier	-	-	-	-	-	-	-
Pgg bij oud papier gezet	-	-	-	-	-	-	-
Pgg door storing (tijdelijk) niet beschikbaar	-	-	-	-	-	-	-
Overig	-	-	-	-	-	28	3
	0	0	0	0	0	59	14

Ontvangstbevestiging

Uw verzoek tot het intrekken van een melding is succesvol verstuurd. Als uw verzoek niet meteen kan worden verwerkt, bijvoorbeeld omdat het meldingsnummer dat u heeft opgegeven niet bekend is bij de Autoriteit Persoonsgegevens, dan ontvangt u daarover zo spoedig mogelijk bericht.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	21-10-2020 08:43:39

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	
Wat is het meldingsnummer van de oorspronkelijke melding?	892be495-da8f-4256-8b99-be217e0c4063
Wat is de reden van intrekking?	Ik trek de melding in omdat uit nader onderzoek is gebleken dat de betreffende mail met voldoende beveiliging (TLS 1.2 en AES256) is verzonden, zodat er geen sprake meer is van een hoog risico als bedoeld in artikel 33 AVG. De inbreuk blijft wel geregistreerd in ons interne datalekregister.

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Gemeente Dantumadiel

Wie meldt het datalek?

Naam	5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e @noardeast-fryslan.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 0271B30D-5943-478D-A5C8-BD63F6FD9F68

Melddatum: 20 september 2022

Meldtijdstip: 14:48

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer (indien van toepassing)	50820753
Naam van het bedrijf of de organisatie	Gemeente Dantumadiel
Adres	Hynsteblom 4
Postcode	9104BR
Plaats	Damwâld

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e@noardeast-fryslan.nl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	9-9-2022
(Mogelijke) einddatum van de inbreuk	20-9-2022
4.2 Wanneer is het incident ontdekt?	20-9-2022
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	Ontvanger van de brief heeft contact met ons opgenomen dat hij een brief had ontvangen die niet voor hem bestemd was.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd dat de persoonsgegevens vernietigd zijn, of zijn de persoonsgegevens teruggestuurd?	Ja

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Gemeente heeft van DJI bericht ontvangen over einde detentie van een inwoner. De coördinator Nazorg gedetineerden heeft deze persoon op het van DJI verkregen adres een brief verstuurd voor het nazorgaanbod. De brief is echter gericht aan de vader van de ex-gedetineerde. De coördinator heeft alleen bij vader aangegeven

dat de brief waarschijnlijk voor een andere persoon bestemd was (een persoonscheck gedaan middels het opvragen van geboortedatum van vader). Daarbij bij vader navraag gedaan of er inwonende op het adres zijn zoals een zoon of een neef. Vader gaf daarop aan een zoon te hebben	maar hier geen contact mee te hebben. Ik heb verder geen navraag gedaan naar adres van zoon gezien privacy / datalek. Vader weet dus niet dat zoon vast heeft gezeten, maar heeft mogelijk door de brief nu wel vermoedens hiervan.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Gegevens van één persoon.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	(Vermoedelijk, maar adres onbekend) inwoner van de gemeente
7.3 Is het exacte aantal betrokkenen bekend?	Ja
Het exacte aantal is:	1

AUTORITEIT PERSOONSGEGEVENS

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Discriminatie of uitsluiting

[✓] Reputatieschade

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Ontvanger (vader) geeft aan geen contact te hebben met zijn zoon, was dus mogelijk of vermoedelijk niet op de hogte van de detentie. Geen contact duidt al op een verstoorde relatie tussen ouder en kind.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee

AUTORITEIT PERSOONSGEGEVENS

Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Adres betrokkene is onbekend. Het adres dat wij van DJI hebben ontvangen klopt niet.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nee, want:
Toelichting:	Niet herstelbaar.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Medewerker gewezen op zorgvuldigheid.

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.

- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	17-10-2022

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

AUTORITEIT
PERSOONSGEGEVENS

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 0271B30D-5943-478D-A5C8-BD63F6FD9F68

Melddatum: 17 oktober 2022

Meldtijdstip: 13:44

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	0271B30D-5943-478D-A5C8-BD63F6FD9F68

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e @noordeast-fryslan.nl
Telefoonnnummer	5.1.2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Het adres van de betrokkene is nog steeds onbekend. Het adres dat wij van DJI hebben ontvangen klopt niet. DJI heeft geen ander adres van betrokkene. In de BRP staat hij nog steeds op dat adres ingeschreven.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de Privacyverklaring van de AP

Opbouw Dantumadiel 2024

Toezicht Algemene Verordening Gegevensbescherming / Wet politiegegevens

Bevindingen en aanbevelingen van de Functionaris Gegevensbescherming

gemeente dantumadiel

Inhoud

Waar in dit document de term ‘verwerkingsverantwoordelijke’ wordt gebruikt betreft dit het college van B&W, de burgemeester of de gemeenteraad, ieder voor de eigen taken en verantwoordelijkheden.

Inleiding

De Algemene Verordening Gegevensbescherming (AVG) stelt eisen aan een rechtmatige verwerking van persoonsgegevens. De overheid heeft hierin een belangrijke voorbeeldfunctie. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties.

De AVG beschrijft het wettelijk kader voor het verwerken van persoonsgegevens. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak.

De AVG raakt vrijwel alle processen van de van gemeente. Dit vloeit voort uit de taken die de gemeente voor inwoners en andere betrokkenen uitvoert. Het aantoonbaar voldoen aan de AVG draagt in belangrijke mate bij aan een betrouwbare overheid. Organisaties moeten aan kunnen tonen dat zij aan de wettelijke vereisten voldoen. De kern van deze verantwoordingsplicht is voor de verwerkingsverantwoordelijke om voorafgaand aan, tijdens en ná de verwerking van persoonsgegevens aantoonbaar een passende set van organisatorische, procedurele en technische maatregelen te hebben toegepast.

De Functionaris Gegevensbescherming (FG) is binnen de gemeente Dantumadiel belast met het houden van onafhankelijk toezicht op de naleving van de AVG en Wpg. Tot de taken van de FG behoort ten minste het (gevraagd én ongevraagd) adviseren en informeren van de verwerkingsverantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving en het toezien op de naleving daarvan. De FG brengt rechtsreeks verslag uit aan de hoogste leidinggevende.

Na de ontvlechting van Noardeast-Fryslân kan Dantumadiel niet meer steunen op de privacy-organisatie van de centrumregeling. In dit verslag beschrijf ik wat nodig is om van Dantumadiel een organisatie te maken die de basisbeginselen voor gegevensbescherming op orde heeft.

5.1.2e

5.1.2e .2e

November 2023

1 Aanbevelingen

Gegevensbescherming is geen kwestie van eenmalig een lijst afvinken. Een organisatie moet continu aan de vereisten voldoen. Dit hoofdstuk beschrijft de belangrijkste aanbevelingen. In de volgende hoofdstukken beschrijf ik de bevindingen die tot deze aanbevelingen hebben geleid.

Organiseer en borg gegevensbescherming

De functies en taken voor gegevensbescherming zijn zonder specifieke formatieomvang opgenomen in het formatieontwerp[1]:

- De taken van de FG worden op basis van een dienstverleningsovereenkomst (dvo) uitgevoerd door de gemeente Noardeast-Fryslân. Hiervoor stelt Noardeast-Fryslân 0,4 fte (14,4 uren per week) beschikbaar. In de dvo is opgenomen welke taken Noardeast-Fryslân wel en niet uitvoert.
- De uitvoerende taken van de privacy-officer (PO) zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.
- Het is raadzaam om per team ten minste één persoon aan te wijzen die het aanspreekpunt is binnen dat team zodat deze als eerste lijn kunnen optreden bij aangelegenheden met betrekking tot informatiebeveiliging en gegevensbescherming/privacy (IB&P). Deze sleutelpersonen, die deze rol naast hun reguliere werkzaamheden in hun takenpakket hebben, komen vervolgens regelmatig bijeen om hun bevindingen op het gebied van IB&P te bespreken. Op deze wijze blijven de FG, PO en CISO op de hoogte van de ontwikkelingen op de werkvloer.

Breng de basis op orde

Het is belangrijk dat Dantumadiel zo snel mogelijk begint om de basis op orde te krijgen. Dat betekent dat ten minste de registers van verwerkingsactiviteiten onder de AVG en Wpg volledig en actueel worden en blijven. Gegevensbescherming moet in beleid, werkprocessen, -instructies en richtlijnen een duidelijke plek krijgen.

Dantumadiel kan zich niet volledig baseren op de registers en processen van de centrumregeling. Zoals in eerdere jaarrapportages is geconcludeerd had en heeft de centrumregeling onvoldoende zicht op alle verwerkingen van persoons- en politiegegevens en de risico's die daarbij kunnen optreden. Het ligt niet in de lijn der verwachtingen dat hier in de resterende maanden van 2023 nog een significante verbetering op zal treden.

[1] Het formatieontwerp zoals dat op 25 april 2023 door het college van b&w van Dantumadiel is vastgesteld.

Een aantal taken wordt niet uit eigen formatie ingevuld, maar door Noardeast-Fryslân via een dienstverleningsovereenkomst. Bij een aantal taken is sprake van verwerking van persoonsgegevens. Dantumadiel is en blijft verantwoordelijk voor de verwerking van deze persoonsgegevens. Afhankelijk van de taak en vorm kan de dienstverlener verwerker of samen met Dantumadiel gezamenlijk verwerkingsverantwoordelijk zijn. De verantwoordelijkheden van partijen moeten vastgelegd worden.

In de volgende tabel worden de status van de belangrijkste basisverplichtingen getoond.

	AVG	Wpg
Functionaris Gegevensbescherming		
Privacybeleid		
Register van verwerkingsactiviteiten, werkprocessen		
Verwerkers en verwerkersovereenkomsten		
Behandelen datalekken, meldplicht		
Behandelen verzoeken van betrokkenen		

Aanbevelingen

- Creëer voldoende structurele formatie voor een privacy-officer.
- Wijs in ieder team ten minste één persoon aan die voor dat team het aanspreekpunt voor IB&P-aspecten is.
- Geef IB&P een duidelijke plek in beleid, werkprocessen, instructies en richtlijnen.

Actiepunten

- Evalueer het privacybeleid en pas dit zonodig aan. Neem hierbij ook de Wpg-eisen mee.
- Stel de registers van verwerkingsactiviteiten voor AVG- en Wpg-verwerkingen op.
- Het college moet een FG-Wpg aanwijzen.

2 Basisverplichtingen onder de AVG

De AVG bevat verplichtingen waar de verwerkingsverantwoordelijke moet voldoen om aan te tonen dat zij handelt in overeenstemming met de regelgeving. In dit hoofdstuk lopen we langs die verplichtingen.

Bescherming van persoonsgegevens (privacy) is een internationaal grondrecht. De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die dit grondrecht bewaakt. De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Onder toezicht vallen diverse taken, zoals onderzoek doen en behandelen van privacyklachten. De AP is bevoegd om overtredingen te sanctioneren, bijvoorbeeld door een boete of dwangsom op te leggen.

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de AVG, en kan dat aantonen (verantwoordingsplicht). Hij moet daarvoor passende technische en organisatorische maatregelen treffen die hij periodiek evalueert en zonodig actualiseert.

Waar in dit hoofdstuk de term 'verwerkingsverantwoordelijke' wordt gebruikt betreft dit het college van B&W, de burgemeester of de gemeenteraad, ieder voor de eigen taken en verantwoordelijkheden.

2.1 Functionaris Gegevensbescherming

Het college van B&W van Dantumadiel heeft mij op 19 april 2019 als Functionaris Gegevensbescherming aangewezen. De gemeenteraad van Dantumadiel heeft mij op 28 mei 2019 aangewezen als Functionaris Gegevensbescherming. De AP heeft de aanwijzingen geregistreerd als FG000024.

De taken van de FG worden op basis van een dienstverleningsovereenkomst (dvo) uitgevoerd door de gemeente Noardeast-Fryslân. Hiervoor stelt Noardeast-Fryslân 0,4 fte (14,4 uren per week) beschikbaar. In de dienstverleningsovereenkomst is vastgelegd dat de taken en activiteiten in ieder geval de (minimaal) vereiste taken van de Functionaris Gegevensbescherming (FG) zoals genoemd in de artikelen 37 tot en met 39 van de AVG, uitgewerkt in de Richtlijnen voor functionarissen voor Gegevensbescherming (WP243) en artikel 36 Wet politiegegevens (Wpg), behelzen. Hieronder wordt kortgezegd verstaan:

a. Toezicht op naleving van de AVG en de Wpg en beleid met betrekking tot de bescherming van persoonsgegevens;
b. Het informeren en adviseren over verplichtingen op grond van gegevensbeschermingsrecht;
c. Het adviseren over Data Protection Impact Assessments (DPIA's) en toezien op de uitvoering hiervan;
d. Het optreden als contactpersoon voor de Autoriteit Persoonsgegevens (AP).

De FG kan andere taken en plichten vervullen zolang deze niet tot een belangenconflict leiden. Dit betekent dat een FG geen uitvoerende privacytaken kan uitvoeren omdat hij dan toezicht moet houden op zijn eigen werk. De Autoriteit Persoonsgegevens (AP) heeft dit jaar aan twee gemeenten opheldering gevraagd over een mogelijke belangenverstrengeling. Door de FG- en PO-functies door één persoon te laten uitvoeren overtreedt de gemeente mogelijk de wet[2]. Een woordvoerder van de AP noemt het een situatie waarin de slager zijn eigen vlees keurt.

De Informatiebeveiligingsdienst (IBD/VNG) heeft een handreiking voor het functieprofiel van de FG vastgesteld. De Autoriteit Persoonsgegevens heeft in een visiedocument de uitgangspunten voor de rollen, processen en verantwoordelijkheden van de FG opgesteld.

- Handreiking functieprofiel Functionaris Gegevensbescherming[3] (IBD 2023)
- Visiedocument Autoriteit Persoonsgegevens: Positionering van de FG, uitgangspunten voor rollen, processen en verantwoordelijkheden[4] (AP 2022)

2.1.1 Privacy-officer

Het formatieplan kent geen specifieke formatie voor een privacy-officer (PO). Deze functie draagt bij aan privacy compliance van de gemeente. De PO heeft een uitvoerende rol en is verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid van de gemeentelijke organisatie en het ondersteunen van de uitvoering. Dit doet hij in nauwe samenwerking met de FG en de CISO.

De uitvoerende taken en werkzaamheden van de PO vallen niet onder de Overeenkomst en worden derhalve verzorgd door de gemeente Dantumadiel. Dit zijn in ieder geval:

a. Het opstellen van beleid, werkinstructies en richtlijnen (zie §2.2, §2.3 en §3.3);
b. Het behandelen van datalekken (zie §2.5 en §3.5);
c. Het adviseren op specifieke verwerkingen en projecten;
d. Het meewerken aan de uitvoering van Data Protection Impact Assessments (DPIA's) (zie §2.4 en §3.4));

[2] Artikel 38 lid 6 AVG: De functionaris voor Gegevensbescherming kan andere taken en plichten vervullen. De verwerkingsverantwoordelijke of de verwerker zorgt ervoor dat dat deze taken en plichten niet tot een belangenconflict leiden.

[3] https://www.informatiebeveiligingsdienst.nl/product/handreiking-functieprofiel-functionaris-gegevensbescherming-fg/

[4] https://www.autoriteitpersoonsgegevens.nl/uploads/imported/positionering_van_de_fg.pdf

e. Het behandelen van de uitgeoefende rechten als bedoeld in hoofdstuk III AVG en paragraaf 4 Wpg door de betrokkene (zie §2.6 en §3.6).

De uitvoerende taken van de PO zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.

Aanbeveling
- Creëer structurele formatie voor een privacy-officer.

De Informatiebeveiligingsdienst (IBD/VNG) heeft een handreiking voor het functieprofiel van de PO vastgesteld.
- Handreiking functieprofiel Privacy Officer[5] (IBD 2023)

2.1.2 Privacysleutelpersonen
Het is raadzaam om per team ten minste één persoon aan te wijzen die het privacy aanspreekpunt is binnen het team zodat deze als eerste lijn kan optreden bij privacyvragen. Al deze privacysleutelpersonen, die privacy naast hun reguliere werkzaamheden in hun takenpakket hebben, komen vervolgens regelmatig bijeen om hun bevindingen op het gebied van privacy te bespreken. Op deze wijze blijft de FG op de hoogte van de ontwikkelingen op de werkvloer.

VNG Connect biedt een online basiscursus[6] aan voor gemeentelijke privacy ambassadeurs, juristen, beleidsmedewerkers of anderszins medewerkers met een vergaande interesse in privacy. Deze cursus kan een mooie opstap zijn om een actievere rol te gaan spelen binnen de gemeente op het gebied van privacy.

2.2 Privacybeleid
Op 29 mei 2018 heeft de gemeenteraad van Dantumadiel de Privacyverordening vastgesteld. Op 27 maart 2018 heeft het college van B&W van Dantumadiel privacybeleid vastgesteld.

Het is van belang dat de organisatie periodiek beoordeelt of het beleid nog aansluit bij interne en externe ontwikkelingen. Het beleid moet daarom ten minste eens per drie jaar geëvalueerd en waar nodig aan te passen. Het beleid is na de vaststelling in 2018 niet geëvalueerd.

Opstellen van privacybeleid is een taak van de PO. De uitvoerende taken van de PO zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.

Aanbeveling
- Wijs in ieder team ten minste één persoon aan die voor dat team het aanspreekpunt voor IB&P-aspecten is.

2.3 Register van verwerkingsactiviteiten
De verwerkingsverantwoordelijke moet op grond van artikel 30 AVG een register van verwerkingsactiviteiten bijhouden van alle verwerkingen van persoonsgegevens die onder zijn verantwoordelijkheid plaatsvinden.

Zoals in de voorgaande jaarverslagen is geconstateerd was en is het register van verwerkingsactiviteiten binnen de centrumregeling niet volledig en niet actueel. In 2021 is hiervoor een inhaalslag gestart, maar deze is door diverse oorzaken, waaronder de organisatieontwikkelingen rondom de wijziging van de hoofdstructuur en de ontvlechting, in 2022 vrijwel geheel tot stilstand gekomen. Het ligt niet in de lijn der verwachtingen dat hier in de laatste maanden van 2023 nog een significante verbetering op zal treden.

Een aantal taken voert Dantumadiel niet zelf uit, maar door Noardeast-Fryslân op basis van een dienstverleningsovereenkomst. Bij een aantal taken is sprake van verwerking van persoonsgegevens. Afhankelijk van de taak kan de dienstverlener verwerker of samen met Dantumadiel gezamenlijk verwerkingsverantwoordelijk zijn. Afhankelijk van die privacypositie moeten de verantwoordelijkheden van partijen vastgelegd worden in verwerkingsovereenkomsten en dergelijke.

Aanbevelingen
- Geef IB&P een duidelijke plek in beleid, werkprocessen, instructies en richtlijnen.

2.4 Data Protection Impact Assessments
Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'.

[5] https://www.informatiebeveiligingsdienst.nl/product/handreiking-functieprofiel-privacy-officer-po/

[6] https://www.vngconnect.nl/academie/Training/Online-basiscursus-AVG/ddb6b93a-93ca-4c9d-a6f3-1005d8ee0a99

Zoals in de voorgaande jaarverslagen is geconstateerd was het register van verwerkingsactiviteiten binnen de centrumregeling niet volledig en niet actueel. Hetzelfde geldt voor de DPIA's. Ook hierbij ligt het niet in de lijn der verwachtingen dat hier in de laatste maanden van 2023 nog een significante verbetering op zal treden.

Het uitvoeren van een DPIA past niet in de wettelijke taken van de FG en kan mogelijk tot een belangenconflict leiden: de FG moet immers toezicht houden op de naleving van de AVG, waaronder de uitvoering van DPIA's.

Het meewerken aan de uitvoering van DPIA's is een taak van de PO. De uitvoerende taken van de PO zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.

2.5 Registratie en meldplicht datalekken

De verwerkingsverantwoordelijke moet ernstige datalekken binnen 72 uur "nadat hij er kennis van heeft genomen" melden aan de Autoriteit Persoonsgegevens en de betrokkenen. Daarom is het belangrijk dat een datalekmelding meteen wordt opgepakt. In verband met de daaraan verbonden meldtermijnen moet iemand meteen kunnen laten vallen waar hij mee bezig is om de datalekmelding in behandeling te nemen.

Het behandelen van een datalek past niet in de wettelijke taken van de FG en kan mogelijk tot een belangenconflict leiden: de FG moet immers toezicht houden op de naleving van de AVG, waaronder de (tijdige) behandeling van datalekken.

Het behandelen van datalekken is een taak van de PO. De uitvoerende taken van de PO zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.

2.6 Rechten van betrokkenen, bezwaarschriften en klachten

Betrokkenen hebben in de AVG rechten gekregen om te weten wat een verwerkingsverantwoordelijke met zijn persoonsgegevens doet. Het gaat om het inzagerecht, het recht op rectificatie, gegevenswissing, beperking van de verwerking, en bezwaar.

De verwerkingsverantwoordelijk moet "onverwijld en in ieder geval binnen een maand" reageren op een dergelijk verzoek. In verband met die termijn moet iemand meteen kunnen laten vallen waar hij mee bezig is om een verzoek in behandeling te nemen.

Het behandelen van een rechtenverzoek, bezwaarschriften en klachten past niet in de wettelijke taken van de FG en kan mogelijk tot een belangenconflict leiden: de FG moet immers toezicht houden op de naleving van de AVG, waaronder de behandeling van verzoeken, bezwaarschriften en klachten.

Het behandelen van uitgeoefende rechten als bedoeld in hoofdstuk III AVG en paragraaf 4 Wpg door de betrokkene is een taak van de PO. De uitvoerende taken van de PO zijn toegevoegd aan de functie Businesscontroller. Dit leidt tot een risico dat de PO-taken niet de aandacht krijgen die deze nodig hebben. Daarnaast bestaat een risico dat medewerkers die de functie van businesscontroller vervullen onvoldoende kennis van het werkveld gegevensbescherming hebben en houden.

3 Basisverplichtingen onder de Wpg

De Wet politiegegevens (Wpg) bevat verplichtingen waar de verwerkingsverantwoordelijke moet voldoen om aan te tonen dat zij handelt in overeenstemming met de regelgeving. In dit hoofdstuk lopen we langs die verplichtingen.

Voor de Wpg is de verwerkingsverantwoordelijke de werkgever van de boa. Voor gemeenten is dat het college van burgemeester en wethouders. Voor de ontvlechting was Noardeast-Fryslân de werkgever van boa's die ook voor Dantumadiel werkten. Dantumadiel wordt vanaf 2024 ook als verwerkingsverantwoordelijke voor de Wpg aangemerkt omdat er volgens het formatieplan ook zelf boa's met opsporingstaken in dienst zijn.

De Wpg is 'strenger' dan de AVG. Zo kent de Wpg auditverplichtingen. Ieder jaar moet een interne audit plaatsvinden op één of meer onderdelen van de wet. Iedere vier jaar moet een externe audit plaatsvinden waarvan de resultaten gedeeld moeten worden met de Autoriteit Persoonsgegevens. Daarnaast bevat de Wpg een explicitiete documentatieplicht.

3.1 Functionaris Gegevensbescherming

De verwerkingsverantwoordelijke moet op grond van artikel 36 Wpg een functionaris gegevensbescherming aanwijzen. De taken en bevoegdheden van de Wpg-FG zijn vrijwel identiek aan die van de AVG-FG.

Dantumadiel heeft vanaf 2024 zelf boa's met opsporingstaken in dienst. Dat maakt het college verwerkingsverantwoordelijk voor verwerkingen van politiegegevens op grond van de Wpg. Het college zal daarom een Wpg-FG aan moeten wijzen.

3.2 Privacybeleid

Er is geen specifiek privacybeleid waarin de vereisten van de Wpg zijn opgenomen.

3.3 Register van verwerkingsactiviteiten

De verwerkingsverantwoordelijke moet op grond van artikel 31d Wpg een register van verwerkingsactiviteiten bijhouden van alle verwerkingen van persoonsgegevens die onder zijn verantwoordelijkheid plaatsvinden.

Er is geen register van verwerkingsactiviteiten dat de verwerkingen van politiegegevens op grond van de Wpg beschrijft.

De Wpg bevat daarnaast in artikel 32 een expliciete documentatieplicht om de doelen van een verwerking, en de verstrekking van politiegegevens schriftelijk vast te leggen.

3.4 Data Protection Impact Assessments

Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is op grond van artikel 4c verplicht voor 'risicovolle verwerkingen'.

3.5 Registratie en meldplicht datalekken

De verwerkingsverantwoordelijke moet in datalekken binnen 72 uur "nadat hij er kennis van heeft genomen" melden aan de Autoriteit Persoonsgegevens[7]. Daarom is het belangrijk dat een datalekmelding meteen wordt opgepakt. Het behandelen van een datalek past niet in de wettelijke taken van de FG en kan mogelijk tot een belangenconflict leiden: de FG moet immers toezicht houden op de naleving van de AVG, waaronder de tijdige en correcte behandeling van datalekken.
Dat betekent dat een andere functie meldingen van datalekken moet behandelen. In verband met de daaraan verbonden termijnen moet iemand meteen kunnen laten vallen waar hij mee bezig is om de datalekmelding in behandeling te nemen.

3.6 Rechten van betrokkenen, bezwaarschriften en klachten

Betrokkenen hebben in de Wpg rechten gekregen om te weten wat een verwerkingsverantwoordelijke met zijn persoonsgegevens doet. Het gaat om het inzagerecht, het recht op rectificatie en gegevenswissing. De verwerkingsverantwoordelijk moet binnen een maand aan een dergelijk verzoek voldoen.

3.7 Audits

De Wpg kent een auditregime[8]. Het college moet ieder jaar een interne audit (laten) uitvoeren op een of meer onderdelen van de wet[9]. En iedere vier jaar een externe privacy-audit (laten) uitvoeren op de volledige wet[10]. De eerstvolgende externe privacy-audit ziet op de periode 1 januari 2022 tot en met 31 december 2025. Het college moet de resultaten van de externe privacy-audits delen met de Autoriteit Persoonsgegevens.

Dantumadiel zal vanaf 2024 ieder jaar een interne audit moeten (laten) uitvoeren, en in 2025 een externe privacy-audit. De Wpg verbindt bepaalde eisen aan de auditor. Dantumadiel beschikt voor zover bekend niet over een auditor die aan die eisen voldoet. Er zal daarom een auditor ingehuurd moeten worden.

[7] Artikel 33a Wpg
[8] Artikel 33 Wpg, artikel 6.5 Besluit politiegegevens
[9] Artikel 3 Regeling Periodieke Audit Politiegegevens
[10] Artikel 2 Regeling Periodieke Audit Politiegegevens

Bijlage: verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Dit is de externe toezichthouder binnen Nederland met betrekking tot de uitvoering van gegevensbescherming. Voor meer informatie zie www.autoriteitpersoonsgegevens.nl.

AVG/GDPR
Dit is de Europese verordening. AVG staat voor Algemene Verordening Gegevensbescherming. GDPR (General Data Protection Regulation) is de internationale benaming van de Verordening.

Betrokkene(n)
De perso(o)n(en) waarvan de persoonsgegevens worden verwerkt.

Datalek
Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens, zonder dat dit de bedoeling is. Er is dus sprake van een datalek als er persoonsgegevens in handen vallen van personen of organisaties die geen toegang tot die gegevens zouden mogen hebben. Ook wanneer persoonsgegevens verloren zijn geraakt, is er een datalek. De meest voorkomende datalekken betreffen verkeerd verstuurde e-mail.

Datalek, meldplicht
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen, moet de gemeente het datalek binnen 72 uur na ontdekkingmelden bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.
Gemeenten moeten betrokkene(n) informeren over een datalek wanneer het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene(n) zodat zij eventueel voorzorgsmaatregelen kunnen treffen.

Datalek, register
De gemeente moet alle datalekken documenteren in een register: het datalekkenregister. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of de gemeente aan de meldplicht heeft voldaan.

DPIA (Data Protection Impact Assessment)
Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De Avg geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren. De Nederlandse term is 'gegevensbeschermingseffectbeoordeling' (GEB).

Functionaris (voor) Gegevensbescherming (FG)
De FG houdt het toezicht binnen een organisatie op de correcte uitvoering van de verwerking volgens de AVG. Een FG is verplicht bij overheden en publieke organisaties.

IB&P
Informatiebeveiliging (IB) en privacy (P) zijn sterk met elkaar verbonden. Zonder beveiliging kan er geen sprake zijn van bescherming van persoonsgegevens.

Persoonsgegeven
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Daar is al snel sprake van: naam, (mail)adres, woonplaats, geboortedatum, geslacht, functie, inhoud van e-mails, surfgedrag, loginnamen, wachtwoorden, IP- adressen, tracking cookies enz. enz. Niet alleen geschreven tekst kan een persoonsgegeven zijn, ook beeld en geluid kunnen persoonsgegevens zijn.

Politiegegevens
Politiegegevens zijn persoonsgegevens die op basis van de Wet politiegegevens (Wpg) worden verwerkt.

Privacy by design
Privacy by design betekent dat er bijvoorbeeld bij het ontwerpen van een informatiesysteem of nieuw product rekening gehouden wordt met privacy (design). Het is een wettelijke verplichting onder de Avg. Los daarvan vergt het doen van aanpassingen achteraf vaak meer kosten en inspanning dan wanneer privacy vriendelijke maatregelen al tijdens de ontwikkelfase zijn geïmplementeerd en toegepast. Het devies is ook daarom om in een zo vroeg mogelijk stadium in vulling te geven aan de Avg verplichtingen. Met andere woorden: het pro-actief borgen van gegevensbescherming in beleid, procedures en processen.

Rechten van betrokkenen
Onder de Avg hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om de navolgende rechten:
- Het recht op inzage: het recht van mensen om de persoonsgegevens die de gemeente van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling: het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen.

- Het recht op verwijdering: het desgevraagd wissen van persoonsgegevens van betrokkene.
- Het recht op vergetelheid: het recht om ‘vergeten’ te worden. Dat wil zeggen dat iedere koppeling naar of kopie van de gegevens worden gewist.
- Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- In de situatie van geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
- Het recht op dataportabiliteit: het recht om persoonsgegevens over te dragen. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op duidelijke informatie over wat de gemeente met hun persoonsgegevens doet.

Verantwoordingsplicht
De Avg legt de verantwoordelijkheid bij de gemeente als organisatie om aan te tonen dat de gemeente aan de privacyregels voldoet. Verantwoordelijkheid is het vermogen om compliance met de Avg aan te tonen. Dit is dus voor verantwoordelijken en verwerkers verplicht. De verantwoording kan vormgegeven worden door het bijhouden van de verschillende registers: verwerkingsregister, datalekken, verwerkersovereenkomsten etc.

Verwerken / verwerking
Dit is in feite alles wat de gemeente doet met persoonsgegevens. Het omvat de hele levenscyclus van informatie, en alles wat je doet of zou kunnen doen met persoonsgegevens. Bijvoorbeeld: verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, combineren, afschermen of wissen enz. enz.

Verwerker
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt , zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Verwerkersovereenkomst
Dit is een overeenkomst tussen verantwoordelijke en verwerker, waarin de verantwoordelijkheden en afspraken over de verwerking worden vastgelegd. De overeenkomst regelt vaak algemene zaken zoals aansprakelijkheid, plus een bijlage waarin de specifieke kenmerken rondom de verwerking worden benoemd.

(Verwerkings)verantwoordelijke
Dit is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerkingsregister
De gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer de verwerkingsdoeleinden, beschrijving van de categorieën betrokkenen en van de categorieën persoonsgegevens, de beoogde bewaartermijnen (de termijnen waarbinnen de persoonsgegevens moeten worden gewist) en een beschrijving van de wijze waarop de gegevens beveiligd zijn.

Opbouw Dantumadiel 2024-1

Toezicht Algemene Verordening Gegevensbescherming / Wet politiegegevens

Bevindingen en aanbevelingen van de Functionaris Gegevensbescherming

gemeente dantumadiel

2024-144637

Inhoud

Taken en positie FG

De gemeente Dantumadiel en de gemeente Noardeast-Fryslân zijn overeengekomen dat Noardeast-Fryslân een aantal taken, waaronder die van de Functionaris Gegevensbescherming, voor Dantumadiel uitvoert. Hiertoe hebben beide gemeenten op 19 december 2023 een dienstverleningsovereenkomst gesloten. Daarin is vastgelegd dat de taken en activiteiten in ieder geval de (minimaal) vereiste taken van de FG zoals genoemd in de artikelen 37 tot en met 39 AVG van de AVG, uitgewerkt in de Richtlijnen (WP243) en artikel 36 van de Wpg behelzen. Hieronder wordt kort gezegd verstaan:

a. Toezicht op naleving van de AVG en de Wpg en beleid met betrekking tot bescherming van persoonsgegevens;
b. Het informeren en adviseren over verplichtingen op grond van gegevensbeschermingsrecht;
c. Het adviseren over Data Protection Impact Assessments (DPIA's) en toezien op de uitvoering hiervan;
d. Het optreden als contactpersoon voor de Autoriteit Persoonsgegevens.

De uitvoerende taken en werkzaamheden van de Privacy Officer (PO) vallen niet onder de dienstverleningsovereenkomst en worden derhalve verzorgd door de gemeente Dantumadiel. Dit zijn in ieder geval:

a. Het opstellen van beleid, werkinstructies en richtlijnen;
b. Het behandelen van datalekken;
c. Het adviseren op specifieke verwerkingen en projecten;
d. Het meewerken aan de uitvoering van Data Protection Impact Assessments (DPIA's);
e. Het behandelen van uitgeoefende rechten als bedoeld in hoofdstuk III AVG en paragraaf 4 Wpg door de betrokkene.

Organisatiebesluit Dantumadiel 2024, artikel 8

1. Op het gebied van informatieveiligheid en gegevensbescherming gelden als uitgangspunt de door het college vastgestelde kaders ten aanzien van informatieveiligheid en de Europese en landelijke wet- en regelgeving en normenkaders.
2. De directie is op concernniveau verantwoordelijk voor de juiste implementatie van de informatieveiligheidsmaatregelen in de bedrijfsprocessen en in de in- en externe (informatie)systemen. De teammanagers hebben eenzelfde verantwoordelijkheid voor hun eigen teams en zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun teams.
3. De Organisatie kent een Functionaris Gegevensbescherming (FG) als bedoeld in de Algemene Verordening Gegevensbescherming en de Wet politiegegevens, die tot taak heeft toe te zien op en te adviseren omtrent een juiste toepassing van regelgeving en beleid met betrekking tot de bescherming van persoonsgegevens. De FG adviseert en rapporteert vanuit een onafhankelijke positie rechtstreeks aan de directie en/of het college.
4. De Organisatie kent een Chief Information Security Officer (CISO), die verantwoordelijk is voor het actueel houden van het informatieveiligheidsbeleid, het adviseren bij projecten en het initiëren van risicoanalyses. De CISO kan vanuit een onafhankelijke positie rechtstreeks adviseren aan de directie en/of het college. De verdere organisatorische uitwerking van bij de informatieveiligheid betrokken functies, rollen en verantwoordelijkheden vindt plaats in een door de directie vast te stellen nota.

Inleiding

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. De AVG zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens. De overheid heeft hierin een belangrijke voorbeeldfunctie. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties.

De AVG beschrijft het wettelijk kader voor het verwerken van persoonsgegevens. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. De Wet politiegegevens is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsmabtenaar (boa) in het kader van zijn opsporingstaak. De Wpg stelt net als de AVG verschillende eisen aan de verwerkingen, zoals het aanwijzen van een interne toezichthouder, de registers voor verwerkingen en datalekken.

De AVG raakt vrijwel alle processen van de van gemeente. Dit vloeit voort uit de taken die de gemeente voor inwoners en andere betrokkenen uitvoert. Zonder persoonsgegevens kan de gemeente haar taken niet uitvoeren. Het aantoonbaar voldoen aan de AVG draagt in belangrijke mate bij aan een betrouwbare overheid.

Organisaties zijn verantwoordingsplichtig voor naleving van de privacywetgeving: zij moeten aan kunnen tonen dat zij aan de wettelijke vereisten voldoen. De kern is de plicht voor de verwerkingsverantwoordelijke om voorafgaand aan, tijdens en ná de verwerking van persoonsgegevens aantoonbaar een passende set van organisatorische, procedurele en technische maatregelen te hebben toegepast.

De Functionaris Gegevensbescherming. (FG) is binnen de gemeente Dantumadiel belast met het houden van onafhankelijk toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Tot de taken van de FG behoort ten minste het (gevraagd én ongevraagd) adviseren en informeren van de verwerkingsverantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving en het toezien op de naleving daarvan.

De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende. Deze rapportage geeft een beeld van de stand van zaken van de naleving van de AVG en Wpg door de organisatie. Het rapport schetst een aantal belangrijke ontwikkelingen, trends en gebeurtenissen. Daarbij doe ik concrete aanbevelingen voor verdere borging van de compliance. Het gaat daarbij om verwerkingen die onder de verantwoordelijkheid van het college van burgemeester en wethouders, de burgemeester en de gemeenteraad worden uitgevoerd.

Dantumadiel is een organisatie in opbouw. Na de ontvlechting van Noardeast-Fryslân kan Dantumadiel niet meer steunen op de privacy-organisatie van Noardeast-Fryslân. In dit verslag beschrijf ik wat nodig is van Dantumadiel een organisatie te maken die AVG- en Wpg-compliant is.

5.1.2e

5.1.2e

September 2024

1 Belangrijkste bevindingen en aanbevelingen

Gegevensbescherming is geen kwestie van eenmalig een lijst afvinken. Een organisatie moet continu aan de vereisten voldoen. Dit hoofdstuk beschrijft de belangrijkste bevindingen van de FG.

In november 2023 heb ik het Verslag Opbouw Dantumadiel 2024[1] toegezonden aan de directie. In dit verslag heb ik actiepunten benoemd. Op 31 januari 2024 heb ik dit verslag besproken met Govert van Oudenaarden (directie) en 5.1.2e 5.1.2e We hebben daarin onder andere afgesproken dat ik tweemaal per jaar rapporteer aan de directie.

1.1 Basis op orde: register van verwerkingsactiviteiten

Dantumadiel is een organisatie in opbouw. Daarbij moeten ook de basisvereisten voor de AVG en Wpg op orde komen en blijven.

De verwerkingsverantwoordelijks is onder de AVG en de Wpg verplicht[2] om een register van verwerkingsactiviteiten bij te houden. Dit register vermeld welke verwerkingen van persoonsgegevens onder de verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden, voor welke doelen, de categorieën van betrokkenen en categorieën van persoonsgegevens, de bewaartermijnen, en de grondslagen op basis waarvan die persoonsgegevens verwerkt worden. Het register vormt hiermee de basis van de privacyboekhouding.

Deze verwerkingsregisters zijn er op dit moment nog niet

In het Verslag Opbouw Dantumadiel 2024 heb ik als actiepunt het opstellen van de registers van verwerkingsactiviteiten voor de AVG en de Wpg benoemd.

Het is van belang dat Dantumadiel zo snel mogelijk start met de bouw van het register van verwerkingsactiviteiten voor zowel voor de AVG als de Wpg. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens.

1.2 Basis op orde: DPIA

Een volgende stap is om voor iedere verwerking te bepalen of de verwerking een dermate hoog risico voor de rechten en vrijheden van betrokkenen oplevert. Als dat het geval is, dan moet de verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, DPIA) uitvoeren. Hiermee worden de risico's van de verwerkingen in kaart gebracht en kunnen de maatregelen beschreven en geïmplementeerd worden om die risico's zoveel mogelijk weg te nemen. De Autoriteit Persoonsgegevens (AP) heeft in een besluit typen verwerkingen benoemd waarvoor een voorafgaande DPIA verplicht is[3].

Dantumadiel heeft geen zicht op de risico's bij de verwerking van persoonsgegevens

De Autoriteit Persoonsgegevens heeft een aantal typen verwerkingen benoemd waarvoor een DPIA verplicht is gesteld. Er zijn geen DPIA's of quickscans daarvoor uitgevoerd. De organisatie heeft daarom onvoldoende zicht welke de meest risicovolle verwerkingen zijn en welke maatregelen genomen moeten zijn/worden om die risico's weg te nemen.

Het is van belang dat Dantumadiel beoordeelt voor welke verwerkingen van persoons- en politiegegevens een DPIA moet worden uitgevoerd. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens, de risico's die zich daarbij kunnen voordoen en de maatregelen die de organisatie moet nemen om die risico's zoveel mogelijk weg te nemen.

De Informatiebeveiligingsdienst (IBD/VNG) heeft recent de handreiking 'Samen naar een kwalitatief goede DPIA' gepubliceerd[4] met daarbij onder andere sjablonen voor de (pre-)DPIA en een lijst met 'must-have-DPIA's'.

1.3 Auditverplichtingen Wet politiegegevens

De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak. De Wpg verplicht tot jaarlijkse audits op de verwerking van politiegegevens. In deze audits worden opzet, bestaan en werking van 31 beheersingsmaatregelen die borgen dat de verwerkingen aan de Wpg-eisen voldoen getoetst[5].

De afgelopen jaren waren de boa's die voor Dantumadiel werkten in dienst van Noardeast-Fryslân. Vanaf 2024 zijn zij in dienst van Dantumadiel. Het college van burgemeester en wethouders van Dantumadiel is dit jaar voor het eerst zelfstandig auditplichtig (de werkgever van de boa's is verwerkingsverantwoordelijk):

- In 2024 moet er een interne audit op een of meer onderdelen van de wet plaatsvinden.
- In 2025 moet een externe audit op alle onderdelen van de wet plaatsvinden waarvan het college de uitkomsten uiterlijk 31 december 2025 naar de Autoriteit Persoonsgegevens (AP) moet sturen.

[1] Zie 2024-144637
[2] Artikel 30 AVG en artikel 31d Wpg
[3] https://wetten.overheid.nl/BWBR0042812/
[4] https://www.informatiebeveiligingsdienst.nl/product/dpia-handreiking-samen-naar-een-kwalitatief-goede-dpia/
[5] https://www.norea.nl/uploads/bfile/2ea115a8-bb2f-4451-903b-5b0f62d3f9b0

- In de jaren 2026 tot en met 2028 moet ieder jaar een interne audit op een of meer onderdelen van de wet plaatsvinden. In 2029 moet het college opnieuw een extern privacy-audit op alle onderdelen van de wet uitvoeren en de resultaten weer naar de AP sturen.

De AP heeft vorige maand de lat voor de externe audit die we in 2025 moeten doen hoog gelegd[6]: "*Eind 2025 zijn boa-werkgevers opnieuw verplicht om een externe audit te laten uitvoeren naar de omgang met persoonsgegevens. Tegen die tijd hebben deze organisaties meerdere jaren de tijd gehad om te voldoen aan de beheersingsmaatregelen. De AP gaat er bij die ronde daarom van uit dat de boa-werkgevers conform de Wpg omgaan met persoonsgegevens en dit met de audit kunnen aantonen. Wanneer een organisatie hieraan niet (genoeg) voldoet, kan de AP handhavende maatregelen opleggen.*"

Eisen aan auditor

Niet iedereen mag de audits doen. In artikel 5 en 6 van de Regeling periodieke audit politiegegevens (Rpap) staan de eisen vermeld waaraan de auditor moet voldoen. De auditor moet zijn ingeschreven bij de Nederlandse Orde van Register EDP-auditor, onafhankelijk zijn ten opzichte van de gemeente en beschikken over aantoonbare kennis en vaardigheden over informatievoorziening en processen van verwerkingen van politiegegevens en de geldende wet- en regelgeving. Ik vermoed dat Dantumadiel niet iemand in dienst heeft die aan deze eisen voldoet

Schakel zo snel mogelijk een externe auditor in. Omdat alle boa-organisaties (ruim 600) deze periodieke audits moeten laten doen zou ik niet te lang wachten om extern een auditor te contracteren, in ieder geval voor de externe privacy-audit volgend jaar. Daar zit namelijk een deadline op: de AP moet het auditrapport uiterlijk op 31 december 2025 ontvangen (van het college, dus er is ook nog een voorafgaand collegebesluit nodig).

[6] https://www.autoriteitpersoonsgegevens.nl/actueel/privacyproof-werken-boa-werkgevers-iets-verbeterd

Bijlage: verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Dit is de externe toezichthouder binnen Nederland met betrekking tot de uitvoering van gegevensbescherming. Voor meer informatie zie www.autoriteitpersoonsgegevens.nl.

AVG/GDPR
Dit is de Europese verordening. AVG staat voor Algemene Verordening Gegevensbescherming. GDPR (General Data Protection Regulation) is de internationale benaming van de Verordening.

Betrokkene(n)
De perso(o)n(en) waarvan de persoonsgegevens worden verwerkt.

Datalek
Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens, zonder dat dit de bedoeling is. Er is dus sprake van een datalek als er persoonsgegevens in handen vallen van personen of organisaties die geen toegang tot die gegevens zouden mogen hebben. Ook wanneer persoonsgegevens verloren zijn geraakt, is er een datalek. De meest voorkomende datalekken betreffen verkeerd verstuurde e-mail.

Datalek, meldplicht
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen, moet de gemeente het datalek binnen 72 uur na ontdekkingmelden bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.
Gemeenten moeten betrokkene(n) informeren over een datalek wanneer het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene(n) zodat zij eventueel voorzorgsmaatregelen kunnen treffen.

Datalek, register
De gemeente moet alle datalekken documenteren in een register: het datalekkenregister. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of de gemeente aan de meldplicht heeft voldaan.

DPIA (Data Protection Impact Assessment)
Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De Avg geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren. De Nederlandse term is 'gegevensbeschermingseffectbeoordeling' (GEB).

Functionaris (voor) Gegevensbescherming (FG)
De FG houdt het toezicht binnen een organisatie op de correcte uitvoering van de verwerking volgens de AVG. Een FG is verplicht bij overheden en publieke organisaties.

Persoonsgegeven
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Daar is al snel sprake van: naam, (mail)adres, woonplaats, geboortedatum, geslacht, functie, inhoud van e-mails, surfgedrag, loginnamen, wachtwoorden, IP-adressen, tracking cookies enz. enz. Niet alleen geschreven tekst kan een persoonsgegeven zijn, ook beeld en geluid kunnen persoonsgegevens zijn.

Politiegegevens
Politiegegevens zijn persoonsgegevens die de boa op basis van de Wet politiegegevens (Wpg) in de opsporingstaak verwerkt.

Privacy by design en default
Privacy by design betekent dat er bijvoorbeeld bij het ontwerpen van een informatiesysteem of nieuw product rekening gehouden wordt met privacy. Privacy by default betekent dat standaardinstellingen zo privacyvriendelijk mogelijk zijn. Dit zijn wettelijke verplichting onder de Avg. Met andere woorden: het pro-actief borgen van gegevensbescherming in beleid, procedures en processen.

Rechten van betrokkenen
Onder de Avg hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om de navolgende rechten:

- Het recht op inzage: het recht van mensen om de persoonsgegevens die de gemeente van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling: het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen.
- Het recht op verwijdering: het desgevraagd wissen van persoonsgegevens van betrokkene.
- Het recht op vergetelheid: het recht om 'vergeten' te worden. Dat wil zeggen dat iedere koppeling naar of kopie van de gegevens worden gewist.
- Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- In de situatie van geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
- Het recht op dataportabiliteit: het recht om persoonsgegevens over te dragen. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op duidelijke informatie over wat de gemeente met hun persoonsgegevens doet.

Verantwoordingsplicht
De Avg legt de verantwoordelijkheid bij de gemeente als organisatie om aan te tonen dat de gemeente aan de privacyregels voldoet. Verantwoordelijkheid is het vermogen om compliance met de Avg aan te tonen. Dit is dus voor verantwoordelijken en verwerkers verplicht. De verantwoording kan vormgegeven worden door het bijhouden van de verschillende registers: verwerkingsregister, datalekken, verwerkersovereenkomsten etc.

Verwerken / verwerking
Dit is in feite alles wat de gemeente doet met persoons- en politiegegevens. Het omvat de hele levenscyclus van informatie, en alles wat je doet of zou kunnen doen met deze gegevens. Bijvoorbeeld: verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, combineren, afschermen of wissen, et cetera.

Verwerker
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt , zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Verwerkersovereenkomst
Dit is een overeenkomst tussen verantwoordelijke en verwerker, waarin de verantwoordelijkheden en afspraken over de verwerking worden vastgelegd. De overeenkomst regelt vaak algemene zaken zoals aansprakelijkheid, plus een bijlage waarin de specifieke kenmerken rondom de verwerking worden benoemd.

(Verwerkings)verantwoordelijke
Dit is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Bij de gemeente is dit, afhankelijk van de taak, het college, de burgemeerster of de gemeenteraad.

Verwerkingsregister
De gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer de verwerkingsdoeleinden, beschrijving van de categorieën betrokkenen en van de categorieën persoonsgegevens, de beoogde bewaartermijnen (de termijnen waarbinnen de persoonsgegevens moeten worden gewist) en een beschrijving van de wijze waarop de gegevens beveiligd zijn.

Jaarverslag AVG / Wpg 2024

Toezicht Algemene Verordening Gegevensbescherming / Wet politiegegevens

Bevindingen en aanbevelingen van de Functionaris Gegevensbescherming

gemeente dantumadiel

2024-144637

Inhoud

Taken en positie FG

De gemeente Dantumadiel en de gemeente Noardeast-Fryslân zijn overeengekomen dat Noardeast-Fryslân een aantal taken, waaronder die van de Functionaris Gegevensbescherming, voor Dantumadiel uitvoert. Hiertoe hebben beide gemeenten op 19 december 2023 een dienstverleningsovereenkomst gesloten. Daarin is vastgelegd dat de taken en activiteiten in ieder geval de (minimaal) vereiste taken van de FG zoals genoemd in de artikelen 37 tot en met 39 AVG van de AVG, uitgewerkt in de Richtlijnen (WP243) en artikel 36 van de Wpg behelzen. Hieronder wordt kort gezegd verstaan:

a. Toezicht op naleving van de AVG en de Wpg en beleid met betrekking tot bescherming van persoonsgegevens;
b. Het informeren en adviseren over verplichtingen op grond van gegevensbeschermingsrecht;
c. Het adviseren over Data Protection Impact Assessments (DPIA's) en toezien op de uitvoering hiervan;
d. Het optreden als contactpersoon voor de Autoriteit Persoonsgegevens.

De uitvoerende taken en werkzaamheden van de Privacy Officer (PO) vallen niet onder de dienstverleningsovereenkomst en worden derhalve verzorgd door de gemeente Dantumadiel. Dit zijn in ieder geval:

a. Het opstellen van beleid, werkinstructies en richtlijnen;
b. Het behandelen van datalekken;
c. Het adviseren op specifieke verwerkingen en projecten;
d. Het meewerken aan de uitvoering van Data Protection Impact Assessments (DPIA's);
e. Het behandelen van uitgeoefende rechten als bedoeld in hoofdstuk III AVG en paragraaf 4 Wpg door de betrokkene.

Organisatiebesluit Dantumadiel 2024, artikel 8

1. Op het gebied van informatieveiligheid en gegevensbescherming gelden als uitgangspunt de door het college vastgestelde kaders ten aanzien van informatieveiligheid en de Europese en landelijke wet- en regelgeving en normenkaders.
2. De directie is op concernniveau verantwoordelijk voor de juiste implementatie van de informatieveiligheidsmaatregelen in de bedrijfsprocessen en in de in- en externe (informatie)systemen. De teammanagers hebben eenzelfde verantwoordelijkheid voor hun eigen teams en zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun teams.
3. De Organisatie kent een Functionaris Gegevensbescherming (FG) als bedoeld in de Algemene Verordening Gegevensbescherming en de Wet politiegegevens, die tot taak heeft toe te zien op en te adviseren omtrent een juiste toepassing van regelgeving en beleid met betrekking tot de bescherming van persoonsgegevens. De FG adviseert en rapporteert vanuit een onafhankelijke positie rechtstreeks aan de directie en/of het college.
4. De Organisatie kent een Chief Information Security Officer (CISO), die verantwoordelijk is voor het actueel houden van het informatieveiligheidsbeleid, het adviseren bij projecten en het initiëren van risicoanalyses. De CISO kan vanuit een onafhankelijke positie rechtstreeks adviseren aan de directie en/of het college. De verdere organisatorische uitwerking van bij de informatieveiligheid betrokken functies, rollen en verantwoordelijkheden vindt plaats in een door de directie vast te stellen nota.

Inleiding

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. De AVG zorgt voor een verhoogde aandacht voor een rechtmatige verwerking van persoonsgegevens. De overheid heeft hierin een belangrijke voorbeeldfunctie. Gemeenten verwerken immers bij de uitoefening van hun taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties.

De AVG beschrijft het wettelijk kader voor het verwerken van persoonsgegevens. Daarnaast heeft de gemeente ook te maken met tal van privacyregels in sectorspecifieke wetgeving. De Wet politiegegevens is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak. De Wpg stelt net als de AVG verschillende eisen aan de verwerkingen, zoals het aanwijzen van een interne toezichthouder, de registers voor verwerkingen en datalekken.

De AVG raakt vrijwel alle processen van de van gemeente. Dit vloeit voort uit de taken die de gemeente voor inwoners en andere betrokkenen uitvoert. Zonder persoonsgegevens kan de gemeente haar taken niet uitvoeren. Het aantoonbaar voldoen aan de AVG draagt in belangrijke mate bij aan een betrouwbare overheid.

Organisaties zijn verantwoordingsplichtig voor naleving van de privacywetgeving: zij moeten aan kunnen tonen dat zij aan de wettelijke vereisten voldoen. De kern is de plicht voor de verwerkingsverantwoordelijke om voorafgaand aan, tijdens en ná de verwerking van persoonsgegevens aantoonbaar een passende set van organisatorische, procedurele en technische maatregelen te hebben toegepast.

De Functionaris Gegevensbescherming. (FG) is binnen de gemeente Dantumadiel belast met het houden van onafhankelijk toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg). Tot de taken van de FG behoort ten minste het (gevraagd én ongevraagd) adviseren en informeren van de verwerkingsverantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving en het toezien op de naleving daarvan.

De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende. Deze rapportage geeft een beeld van de stand van zaken van de naleving van de AVG en Wpg door de organisatie. Het rapport schetst een aantal belangrijke ontwikkelingen, trends en gebeurtenissen. Daarbij doe ik concrete aanbevelingen voor verdere borging van de compliance. Het gaat daarbij om verwerkingen die onder de verantwoordelijkheid van het college van burgemeester en wethouders, de burgemeester en de gemeenteraad worden uitgevoerd.

Dantumadiel is een organisatie in opbouw. Na de ontvlechting van Noardeast-Fryslân kan Dantumadiel niet meer steunen op de privacy-organisatie van Noardeast-Fryslân. In dit verslag beschrijf ik wat nodig is van Dantumadiel een organisatie te maken die AVG- en Wpg-compliant is.

5.1.2e

Functionaris voor Gegevensbescherming
Maart 2025

Leeswijzer

Hoofdstuk 1 beschrijft het toetsingskader voor het FG-toezicht. Naast het wettelijk kader worden de normen voor het toezicht benoemd: het toetsingskader van de Informatiebeveiligingsdienst (IBD/VNG) en het volwassenheidsmodel van CIP-Overheid.
Hoofdstuk 2 bevat de belangrijkste bevindingen over 2024 en aanbevelingen van de FG op basis van het toetsingskader.
De bijlage Beheersmaatregelen bevat de toetsing van de beheersmaatregelen die nodig zijn om te beoordelen of de basis op orde is. Niet alle 155 beheersmaatregelen zijn getoetst. De implementatie van de maatregelen wordt door middel van iconen weergegeven:

	Groei / verbetering
	Consolidatie: het gewenste niveau is bereikt, er wordt geen verdere actie tot verbetering ingezet.
	Stilstand
	Achteruitgang
	Niet getoetst/ niet van toepassing

1 Toetsingskader

1.1 Wettelijk kader

De wetgeving over gegevensbescherming is gebaseerd op de Europese Algemene Verordening Gegevenbescherming (AVG) die sinds 2018 van kracht is. Een aantal bevoegdheden is uitgewerkt in de Nederlandse Uitvoeringswet AVG (UAVG). Voor de opsporingstaak van bijzonder opsporingsambtenaren (boa's) stelt de Wet politiegegevens de kaders. In verschillende materiewetgeving zijn bepalingen over verwerkingen met persoonsgegevens opgenomen. In gemeentelijk privacybeleid geeft de gemeente aan hoe zij uitvoering geeft aan de eisen die de AVG en de Wpg stellen.

1.2 Borgingsproduct IBD

De Informatiebeveiligingsdienst (IBD/VNG) heeft een toetsingskader opgesteld waarmee gemeenten inzicht kunnen krijgen in de mate waarin zij voldoen aan de AVG[1]. Het kader toetst uitsluitend de onderwerpen die de IBD als noodzakelijk beschouwt om aan de AVG te voldoen. Het uitgangspunt is dan ook dat gemeenten aan álle criteria van het toetsingskader voldoen.

Het toetsingskader is opgebouwd uit zeven thema's waarop getoetst wordt. Een thema gaat over een specifiek onderdeel van de AVG.

Beleid	De organisatie heeft processen en bijbehorende verantwoordelijkheden en risico's in kaart gebracht en vastgelegd in beleidsstukken. Deze stukken moeten voor alle werknemers goed vindbaar en begrijpelijk zijn.
Processen	De organisatie heeft alle processen waarbinnen persoonsgegevens worden verwerkt in kaart gebracht. De beschrijving van deze processen wordt actueel gehouden, werkinstructies worden nageleefd en processen met een hoog risico worden getoetst op juistheid.
Organisatorische Inbedding	De organisatie heeft een FG aangesteld en kan zich voor inhoudelijke vraagstukken tot een intern privacyteam richten. Er wordt doorlopend aan bewustwording gedaan.
Rechten van Betrokkenen	De organisatie voldoet aan alle wettelijke eisen die er zijn op het gebied van rechten van betrokkenen. De organisatie is transparant over hoe en welke persoonsgegevens verwerkt worden.
Samenwerking	De organisatie heeft in kaart gebracht met wie zij samenwerkt en heeft daarbij passende afspraken gemaakt. Deze afspraken worden door de betrokken partijen nageleefd.
Gegevens-bescherming	Hoewel pas echt een volledig beeld kan worden geschetst van de stand van zaken op het gebied van gegevensbescherming middels de Baseline Informatiebeveiliging Overheid, zijn privacy en gegevensbescherming niet geheel van elkaar los te trekken. Een aantal informatiebeveiligingsaspecten met een duidelijke privacycomponent zijn dan ook in dit Borgingsproduct opgenomen. Denk bijvoorbeeld aan de handelswijze bij datalekken. De (C)ISO kan helpen bij het beoordelen van de mate waarin aan de bij dit thema opgenomen maatregelen wordt voldaan. Wanneer deze maatregelen voldoende zijn geïmplementeerd, houdt dat dus niet automatisch in dat de organisatie volledig aan de BIO voldoet.
Verantwoording	De organisatie evalueert de naleving van de AVG en rapporteert over de voortgang.

De thema's zijn onderverdeeld in 28 onderwerpen en 155 beheersmaatregelen. De stelregel is dat de burger recht heeft op passende bescherming van zijn privacy, ongeacht in welke gemeente hij woont. Daarom behoort iedere gemeente volgens de IBD 100% van de criteria uit het toetsingskader na te leven, tenzij zij gemotiveerd kan uitleggen dat een bepaald criterium niet van toepassing is (pas-toe-of-leg-uit). Dan is er sprake van een volwassenheidsniveau waarbij procedures en processen volledig zijn geïmplementeerd en beoordelingen worden uitgevoerd om de doeltreffendheid te beoordelen.

1.3 Volwassenheidsniveau

In correspondentie van de Autoriteit Persoonsgegevens (de nationale toezichthouder, hierna: de AP) in het kader van verscherpt toezicht op een provincie en een gemeente lijkt de AP volwassenheidsniveau 3 van het Privacy Volwassenheidsmodel[2] van het Centrum Informatiebeveiliging en Privacybescherming (hierna: CIP-Overheid) als minimum te hanteren. Op niveau 3 werkt een organisatie organisatiebreed volgens een vastgestelde werkwijze aan privacy en kan zij dit aantonen.

Om deze reden zal, naast het toetsingskader van IBD/VNG, ook het volwassenheidsniveau op basis van het toetsingskader van CIP-Overheid, deel uitmaken van het jaarverslag van de FG.

[1] https://www.informatiebeveiligingsdienst.nl/avg-borgingsproduct-3-0/

[2] https://www.cip-overheid.nl/media/uasdokan/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

2 Belangrijkste bevindingen en aanbevelingen

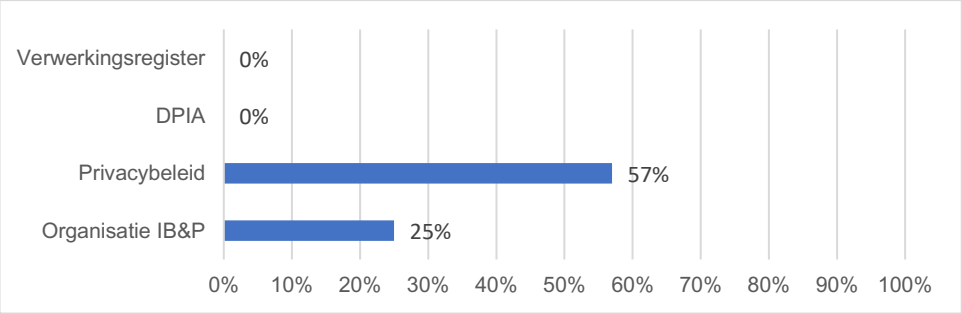
Gegevensbescherming is geen kwestie van eenmalig een lijst afvinken. Een organisatie moet continu aan de vereisten voldoen. Dit hoofdstuk beschrijft de belangrijkste bevindingen van de FG.

In november 2023 heb ik het Verslag Opbouw Dantumadiel 2024 toegezonden aan de directie. In dit verslag heb ik actiepunten benoemd. Op 31 januari 2024 heb ik dit verslag besproken met een directielid en de teammanager Advies en Ondersteuning. We hebben daarin onder andere afgesproken dat ik tweemaal per jaar rapporteer aan de directie.

In september 2024 heb ik het verslag over het eerste halfjaar van 2024 aangeboden aan de directie. Ik heb dat verslag op 14 oktober 2024 besproken/toegelicht in het directie-overleg, en op 4 november 2024 in het MTD (teammanagers en directie).

De stelregel is dat de burger recht heeft op passende bescherming van zijn privacy, ongeacht in welke gemeente hij woont. Daarom behoort iedere gemeente volgens de IBD 100% van de criteria uit het toetsingskader na te leven, tenzij zij gemotiveerd kan uitleggen dat een bepaald criterium niet van toepassing is (pas-toe-of-leg-uit). Dan is er sprake van een niveau waarbij procedures en processen volledig zijn geïmplementeerd en beoordelingen worden uitgevoerd om de doeltreffendheid te beoordelen.

Dantumadiel is een organisatie in opbouw. Daarbij moeten ook de basisvereisten voor de AVG en Wpg op orde komen en blijven. In dit verslag beperkt ik de toetsing daarom tot de thema's en onderwerpen die nodig zijn om te beoordelen of de basis op orde is. Vanuit die basis kan dan aan verdere verbetering gewerkt worden. De volgende grafiek toont de stand aan het einde van het jaar 2024.



2.1 Basis op orde: register van verwerkingsactiviteiten

De verwerkingsverantwoordelijks is onder de AVG en de Wpg verplicht[3] om een register van verwerkingsactiviteiten bij te houden. Dit register vermeld welke verwerkingen van persoonsgegevens onder de verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden, voor welke doelen, de categorieën van betrokkenen en categorieën van persoonsgegevens, de bewaartermijnen, en de grondslagen op basis waarvan die persoonsgegevens verwerkt worden. Het register vormt hiermee de basis van de privacyboekhouding.

Dantumadiel heeft geen register van verwerkingsactiviteiten

Dit betekent dat Dantumadiel geen zicht heeft op de verwerkingen van persoonsgegevens die onder haar verantwoordelijkheid worden uitgevoerd. In het Verslag Opbouw Dantumadiel 2024 heb ik als actiepunt het opstellen van de registers van verwerkingsactiviteiten voor de AVG en de Wpg benoemd. Aan deze aanbeveling is in 2024 geen opvolging gegeven.

Het is van belang dat Dantumadiel zo snel mogelijk start met de bouw van het register van verwerkingsactiviteiten voor zowel voor de AVG als de Wpg. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens.

2.2 Basis op orde: DPIA

Een volgende stap is om voor iedere verwerking te bepalen of de verwerking een dermate hoog risico voor de rechten en vrijheden van betrokkenen oplevert. Als dat het geval is, dan moet de verwerkingsverantwoordelijke een Data Protection Impact Assessment (DPIA) uitvoeren. Hiermee worden de risico's van de verwerkingen in kaart gebracht en kunnen de maatregelen beschreven en geïmplementeerd worden om die risico's zoveel mogelijk weg te nemen. De Autoriteit Persoonsgegevens (AP) heeft in een besluit typen verwerkingen benoemd waarvoor een voorafgaande DPIA verplicht is[4].

Dantumadiel heeft geen zicht op de risico's bij de verwerking van persoonsgegevens

Er zijn geen DPIA's of quickscans uitgevoerd. De organisatie heeft daarom onvoldoende zicht welke de meest risicovolle verwerkingen zijn en welke maatregelen genomen moeten zijn/worden om die risico's weg te nemen.

Het is van belang dat Dantumadiel beoordeelt voor welke verwerkingen van persoons- en politiegegevens een DPIA moet worden uitgevoerd. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens, de risico's die

[3] Artikel 30 AVG en artikel 31d Wpg

[4] https://wetten.overheid.nl/BWBR0042812/

zich daarbij kunnen voordoen en de maatregelen die de organisatie moet nemen om die risico's zoveel mogelijk weg te nemen.

De Informatiebeveiligingsdienst (IBD/VNG) heeft recent de handreiking 'Samen naar een kwalitatief goede DPIA' gepubliceerd[5] met daarbij onder andere sjablonen voor de (pre-)DPIA en een lijst met 'must-have-DPIA's'.

2.3 Basis op orde: beleid

Dantumadiel moet privacybeleid vaststellen dat past bij de verwerkingen die zij uitvoert, en dat moeten zij evalueren en waar nodig actualiseren.

Het beleid is na de vaststelling in 2018 niet meer inhoudelijk geëvalueerd en waar nodig aangepast

Het huidige beleid is in 2018 opgesteld in de periode van de ambtelijke samenwerking van de voormalige DDFK-gemeenten. Vanaf 2019 werden alle taken uitgevoerd in de samenwerking met Noardeast-Fryslân.

Het privacybeleid moet eens per twee jaar geëvalueerd en zo nodig bijgesteld worden. Sinds de eerste vaststelling in 2018 is dit niet gebeurd. Evalueer het beleid, pas het aan op de organisatie van Dantumadiel-2024 en leg het ter vaststelling aan het college van b&w voor.

2.4 Basis op orde: organisatie IB&P

In het beleid zijn rollen, taken en verantwoordelijkheden beschreven die niet of onvoldoende zijn belegd in de organisatie van de gemeente Dantumadiel-2024. Dat betekent dat Dantumadiel niet conform het eigen beleid werkt aan gegevensbescherming.

Dantumadiel werkt niet conform het eigen beleid

Het risico is dat AVG-taken niet of niet goed worden uitgevoerd, of door medewerkers met onvoldoende kennis die nodig is voor die taken.

De IBD heeft eind 2023 de handreiking "Hoe krijg ik een informatiebeveiligings- en privacyteam op sterkte?" gepubliceerd[6]. Om informatiebeveiliging, privacy en gegevensbescherming goed in te bedden en te waarborgen is een sterk IB&P-team van cruciaal belang. De handreiking benoemt essentiële drie functies met bijbehorende profielen: de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de Privacy Officer (PO).

Dantumadiel heeft er bewust voor gekozen om geen formatie voor een privacy-officer te hebben. De uitvoerende taken zijn min of meer informeel belegd bij de CISO en de concerncontrollers. Dit leidt tot het risico dat noodzakelijke werkzaamheden niet, niet tijdig of niet voldoende en met mogelijk onvoldoende kennis uitgevoerd. Denk bijvoorbeeld aan het behandelen van datalekken, inzageverzoeken, opstellen en onderhouden van beleid, werkinstructies, et cetera.

Bouw een IB&P-organisatie waarmee Dantumadiel de uitvoering van de AVG kan schragen. Stel formatie beschikbaar voor een privacy-officer. Zorg dat in ieder team ten minste één aanspreekpunt voor IB&P-onderwerpen is aangewezen, en borg het kennisniveau van deze aanspreekpunten.

2.5 Volwassenheidsniveau

De Autoriteit Persoonsgegevens vindt dat een organisatie minimaal op volwassenheidsniveau 3 moet zitten. Dan werkt een organisatie over de volle breedte aan privacy en kan zij dit aantonen.

Het volwassenheidsniveau van Dantumadiel is volgens het CIP-model (afgerond) 1. Er zijn geen procedures en processen om gegevensbescherming structureel te borgen beschreven en vastgesteld. Gegevensbescherming vindt op verwerkingsniveau informeel plaats. In de bijlage Volwassenheidsniveau wordt deze score uitgelegd. Dantumadiel zal de komende tijd nog de nodige stappen moeten zetten om aantoonbaar tot dat niveau te komen.

2.6 Wet politiegegevens

De Wet politiegegevens (Wpg) is van toepassing op de verwerking van persoonsgegevens door de bijzonder opsporingsambtenaar (boa) in het kader van zijn opsporingstaak. De Wpg verplicht tot jaarlijkse audits op de verwerking van politiegegevens. In deze audits worden opzet, bestaan en werking van 31 beheersingsmaatregelen die borgen dat de verwerkingen aan de Wpg-eisen voldoen getoetst[7].

De afgelopen jaren waren de boa's die voor Dantumadiel werkten in dienst van Noardeast-Fryslân. Vanaf 2024 zijn zij in dienst van Dantumadiel. Het college van burgemeester en wethouders van Dantumadiel is dit jaar voor het eerst zelfstandig auditplichtig (de werkgever van de boa's is verantwoordelijk).

- Over 2024 moet er een interne audit op een of meer onderdelen van de wet plaatsvinden. Deze interne audit heeft nog niet plaatsgevonden.

[5] https://www.informatiebeveiligingsdienst.nl/product/dpia-handreiking-samen-naar-een-kwalitatief-goede-dpia/

[6] https://www.informatiebeveiligingsdienst.nl/product/handreiking-team-op-sterkte/

[7] https://www.norea.nl/uploads/bfile/2ea115a8-bb2f-4451-903b-5b0f62d3f9b0

- In 2025 moet een externe audit over de jaren 2021 tot en met 2024 op alle onderdelen van de wet plaatsvinden waarvan het college de uitkomsten uiterlijk 31 maart 2026 naar de Autoriteit Persoonsgegevens (AP) moet sturen.

De AP heeft de lat voor de resultaten van de externe audit in 2025 hoog gelegd[8]: "*Eind 2025 zijn boa-werkgevers opnieuw verplicht om een externe audit te laten uitvoeren naar de omgang met persoonsgegevens. Tegen die tijd hebben deze organisaties meerdere jaren de tijd gehad om te voldoen aan de beheersingsmaatregelen. De AP gaat er bij die ronde daarom van uit dat de boa-werkgevers conform de Wpg omgaan met persoonsgegevens en dit met de audit kunnen aantonen. Wanneer een organisatie hieraan niet (genoeg) voldoet, kan de AP handhavende maatregelen opleggen.*"

Borg dat de audits voor de Wet politiegegevens tijdig kunnen worden uitgevoerd.

2.7 Diverse onderwerpen

Sectorbeeld Overheid (Autoriteit Persoonsgegevens)

In 2024 heeft de Autoriteit Persoonsgegevens (AP) het "Sectorbeeld Overheid" gepubliceerd[9]. De AP ziet dat de overheid wel stappen zet, maar nog altijd worstelt om aan de privacywetgeving te voldoen.

In het algemeen ziet de AP dat overheidsorganisaties verbeterpunten bij de DPIA's (zie ook §2.2). Deze worden vaak niet of kwalitatief niet goed uitgevoerd. En privacy wordt te vaak nog gezien als slechts een onderdeel van een afweging waarbij andere belangen meer gewicht krijgen. Bestuurders hebben onvoldoende kennis waardoor zij niet altijd de goede besluiten nemen.

Bij gemeenten ziet de AP dat vooral in het sociaal domein, het zorgdomein en het veiligheidsdomein de behoefte bestaat om gegevens met elkaar te delen en aan elkaar te koppelen. Dit mag alleen als daar een juridische grondslag voor is. Bij samenwerkingsverbanden is niet altijd duidelijk welke privacypositie de partijen innemen en wie waarvoor verantwoordelijk is.

Vooral het sociaal domein is kwetsbaar voor AVG-overtredingen. Daar worden veel gevoelige gegevens over gezondheid en de financiële situatie van burgers verwerkt. De wetgeving is niet altijd toereikend om te doen wat in het belang is van de burger. Daarnaast worden in het sociaal domein en bij criminaliteitsbestrijding algoritmes gebruikt om fraude op te sporen en burgers hierop te profileren.

Gemeenten zoeken de grenzen van de AVG en lijken daar vaker overheen te gaan: soms door een gebrek aan kennis, maar ook moedwillig omdat de AVG als belemmering wordt gezien. Aan de andere kant bestaat handelingsverlegenheid omdat de AVG ten onrechte als belemmering wordt zien. Het is vooral voor kleinere gemeenten een opgave om alles over de AVG te weten en deze goed toe te passen.

Gemeenten moeten transparanter zijn over de doelen en manieren waarvoor zij persoonsgegevens van burgers verwerken. Publiceren van het register van verwerkingsactiviteiten en algoritmes kunnen bijdragen aan het verhogen van het vertrouwen in de overheid.

Algoritmeregister

In het Algoritmeregister kunnen overheidsorganisaties algoritmes met impact op burgers publiceren en transparant zijn over hoe zij die inzetten. Registratie is nu nog niet wettelijk verplicht, maar dit wordt naar verwachting in 2025 verplicht. Dantumadiel heeft nog geen algoritmes gepubliceerd[10].

[8] https://www.autoriteitpersoonsgegevens.nl/themas/politie-en-justitie/politie-bijzondere-opsporing-en-justitie/audit-wet-politiegegevens-wpg-audit

[9] https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-overheid

[10] https://algoritmes.overheid.nl/nl/algoritme?organisation=Gemeente+Dantumadiel

BIJLAGE: Volwassenheidsniveau (CIP-Overheid)

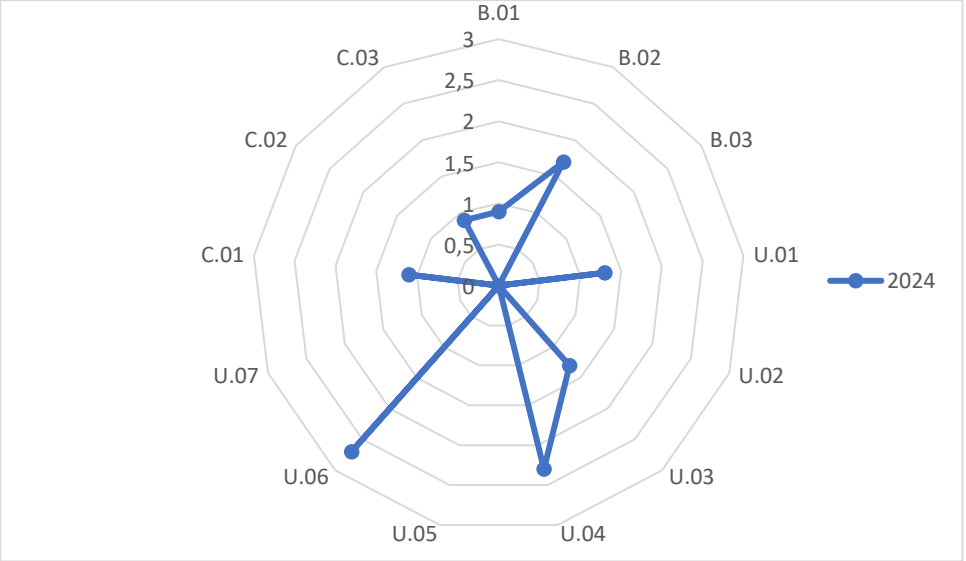
Voldoen aan de privacywet betekent het nemen van de juiste maatregelen in de organisatie en in de techniek. Het volwassenheidsniveau geeft aan hoe volwassen de organisatie is in het borgen van privacy. Het volwassenheidsmodel van het Privacy Volwassenheidsmode[11]l van het Centrum Informatiebeveiliging en Privacybescherming (hierna: CIP-Overheid) kent vijf niveaus die gebruikt kunnen worden om stapsgewijs naar volwassenheid te kunnen groeien. Het volwassenheidsniveau 0, waarbij een organisatie zich niet druk maakt om privacy, beschrijven we hier niet.

1. Informeel: privacy binnen een organisatie is situationeel op verwerkingsniveau is ingericht.
2. Beheerst: grip op privacy is gebaseerd op beslissingen die door meerdere personen gezamenlijk op een vastgelegde wijze worden genomen.
3. Vastgesteld: een organisatie werkt organisatiebreed aan privacy en kan dit conform de wet- en regelgeving aantonen.
4. Voorspelbaar: de organisatie voldoet niet alleen aan de wet- en regelgeving, maar kan er ook actief op wijzigingen anticiperen.
5. Geoptimaliseerd: privacy is een speerpunt op alle niveaus binnen de organisatie en krijgt ook aandacht in communicatie-uitingen naar publiek of klanten.

In correspondentie van de Autoriteit Persoonsgegevens in het kader van het verscherpte toezicht op de provincie Zuid-Holland en de gemeente Eindhoven lijkt de AP volwassenheidsniveau 3 als minimum te hanteren.

De volwassenheidsscore voor Dantumadiel in 2024 is gemiddeld 0,9. De score wordt voornamelijk beïnvloed door de volgende factoren:

- Er is geen actueel geëvalueerd privacybeleid en er zijn geen procesbeschrijvingen, procedures en richtlijnen vastgesteld (B.01).
- Er is geen risicomanagement. Dantumadiel heeft geen register van verwerkingsactiviteitein en heeft daardoor geen inzicht in de risico's die zich bij de verwerking van persoonsgegevens kunnen voordoen en welke maatregelen nodig zijn om die risico zoveel mogelijk weg te nemen (U.02 en B.03).
- Beveiliging van persoonsgegevens is voornamelijk aanwezig door maatregelen die vanuit het Shared Service Centrum Leeuwarden zijn en worden genomen (U.04).
- De bewaartermijnen zijn geïmplementeerd in het zaaksysteem REX. Van veel taakapplicaties is niet bekend of bewaartermijn ingericht zijn of kunnen worden en of persoonsgegevens na afloop van de bewaartermijn worden verwijderd (U.06).



Criterium	2024
B.01 Privacybeleid: de organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld waarin is vastgelegd op welke wijze persoonsgegevens worden verwerkt en invulling wordt gegeven aan de wettelijke beginselen.	0,9
B.02 Organieke inbedding: de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld.	1,7
B.03 Risicomanagement, Privacy by Design en de DPIA: de verwerkingsverantwoordelijke draagt zorg voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen	0,0
U.01 Doelbinding gegevensverwerking: de verwerkingsverantwoordelijke heeft van alle verzamelingen en verwerkingen van persoonsgegevens tijdig, welbepaald en uitdrukkelijk de doeleinden en rechtvaardigingsgronden [grondslagen] omschreven.	1,3
U.02 Register van verwerkingsactiviteiten: de verwerkingsverantwoordelijke en de verwerker hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd. Daarbij geeft het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens.	0,0

[11] https://cip-overheid.nl/media/uasdokan/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

Criterium	2024
U.03 Kwaliteitsmanagement: de verwerkingsverantwoordelijke heeft kwaliteitsmanagement ingericht ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit op verzoek van een betrokkene gebeurt wordt deze over de status van de afhandeling geïnformeerd	1,3
U.04 Beveiligen van de verwerking van persoonsgegevens: de verwerkingsverantwoordelijke en de verwerker treffen technische en organisatorische maatregelen om een verwerking van persoonsgegevens op een passend niveau te beveiligen.	2,3
U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens: de verwerkingsverantwoordelijke stelt bij elke verwerking van persoonsgegevens tijdig en op een vastgelegde en vastgestelde wijze informatie aan de betrokkene beschikbaar, zodat de betrokkene, tenzij een uitzondering geldt, toestemming kan geven voor verwerking.	0,0
U.06 Bewaren van persoonsgegevens: door het treffen van de nodige maatregelen hanteert de organisatie voor persoonsgegevens een bewaartermijn die niet wordt overschreden.	2,7
U.07 Doorgifte persoonsgegevens: bij doorgifte aan een andere verwerkingsverantwoordelijke zijn de onderlinge verantwoordelijkheden duidelijk en bij de doorgifte aan een verwerker zijn er afdoende garanties.	0,0
C.01 Intern toezicht: door of namens de verwerkingsverantwoordelijke vindt evaluatie plaats van de gegevensverwerkingen en is de rechtmatigheid aangetoond.	1,1
C.02 Toegang gegevensverwerking voor betrokkenen: de verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen, tenzij er een specifieke uitzonderingsgrond geldt.	0,0
C.03 Meldplicht datalekken: de verwerkingsverantwoordelijke meldt een datalek binnen de daaraan gestelde termijn aan de AP, documenteert de inbreuk, en informeert de betrokkene, tenzij hiervoor een uitzondering geldt.	0,9

Bijlage: Adviezen, aanbevelingen en opvolging

	Advies / aanbeveling	Status	
Opbouwverslag FG-verslag 2024-1 Managementletter 2024	Het is van belang dat Dantumadiel zo snel mogelijk start met de bouw van het register van verwerkingsactiviteiten voor zowel voor de AVG als de Wpg. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens. Zie ook de opmerkingen van de accountant in de Managementletter 2024: "*U heeft nog geen actueel verwerkingsregister AVG/Wpg. Dit heeft u in de FG-rapportages onder de aandacht gebracht en wordt binnenkort opgepakt door de teammanagers.*"	De FG heeft het register op 2 december 2024 toegelicht in MTD. In 2025 wordt het register gevuld.	
Opbouwverslag FG-verslag 2024-1 Managementletter 2024	Het is van belang dat Dantumadiel beoordeelt voor welke verwerkingen van persoons- en politiegegevens een DPIA moet worden uitgevoerd. Hiermee krijgt de organisatie zicht op de verwerkingen van persoonsgegevens, de risico's die zich daarbij kunnen voordoen en de maatregelen die de organisatie moet nemen om die risico's zoveel mogelijk weg te nemen. Zie ook de opmerkingen van de accountant in de Managementletter 2024: "*De AP heeft voor een aantal typen verwerkingen benoemd waarvoor een DPIA verplicht is. Er zijn in 2024 door Dantumadiel geen DPIA's of quickscans uitgevoerd waardoor het de vraag is of de organisatie voldoende zicht heeft wat de meest risicovolle verwerkingen zijn en welke maatregelen genomen moeten worden om die risico's weg te nemen. Wij adviseren u dit op korte termijn na te gaan.*"		
FG-verslag 2024-1	Borg dat de audits voor de Wet politiegegevens tijdig kunnen worden uitgevoerd.	• Over 2024 moet er een interne audit op een of meer onderdelen van de wet plaatsvinden. Deze interne audit heeft nog niet plaatsgevonden. • In 2025 moet een externe audit over de jaren 2021 tot en met 2024 op alle onderdelen van de wet plaatsvinden waarvan het college de uitkomsten uiterlijk 31 maart 2026 naar de Autoriteit Persoonsgegevens (AP) moet sturen.	
Opbouwverslag Managementletter 2024	Evalueer het privacybeleid en stel dit waar nodig bij. *Zie ook de opmerkingen van de accountant in de Managementletter 2024: "Ook adviseren wij u het privacybeleid te evalueren."*		

Bijlage: verklarende woordenlijst

Autoriteit Persoonsgegevens (AP)
Dit is de externe toezichthouder binnen Nederland met betrekking tot de uitvoering van gegevensbescherming. Voor meer informatie zie www.autoriteitpersoonsgegevens.nl.

AVG/GDPR
Dit is de Europese verordening. AVG staat voor Algemene Verordening Gegevensbescherming. GDPR (General Data Protection Regulation) is de internationale benaming van de Verordening.

Betrokkene(n)
De perso(o)n(en) waarvan de persoonsgegevens worden verwerkt.

Datalek
Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens, zonder dat dit de bedoeling is. Er is dus sprake van een datalek als er persoonsgegevens in handen vallen van personen of organisaties die geen toegang tot die gegevens zouden mogen hebben. Ook wanneer persoonsgegevens verloren zijn geraakt, is er een datalek. De meest voorkomende datalekken betreffen verkeerd verstuurde e-mail.

Datalek, meldplicht
Als een datalek ernstige nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokkenen, moet de gemeente het datalek binnen 72 uur na ontdekkingmelden bij de Autoriteit Persoonsgegevens. Dit wordt de meldplicht van datalekken genoemd.
Gemeenten moeten betrokkene(n) informeren over een datalek wanneer het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor de rechten en vrijheden van de betrokkene(n) zodat zij eventueel voorzorgsmaatregelen kunnen treffen.

Datalek, register
De gemeente moet alle datalekken documenteren in een register: het datalekkenregister. Met deze documentatie moet de Autoriteit Persoonsgegevens kunnen controleren of de gemeente aan de meldplicht heeft voldaan.

DPIA (Data Protection Impact Assessment)
Een DPIA is een instrument om privacy risico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is verplicht voor 'risicovolle verwerkingen'. De Avg geeft aan voor welke categorieën van verwerkingen een DPIA verplicht is. Daarnaast heeft de Autoriteit Persoonsgegevens een aanvullend overzicht opgesteld waarin is geconcretiseerd in welke gevallen de organisatie verplicht is een DPIA uit te voeren. De Nederlandse term is 'gegevensbeschermingseffectbeoordeling' (GEB).

Functionaris (voor) Gegevensbescherming (FG)
De FG houdt het toezicht binnen een organisatie op de correcte uitvoering van de verwerking volgens de AVG. Een FG is verplicht bij overheden en publieke organisaties.

Persoonsgegeven
Een persoonsgegeven is alle informatie, op wat voor manier ook, die iets zegt over een persoon. Daar is al snel sprake van: naam, (mail)adres, woonplaats, geboortedatum, geslacht, functie, inhoud van e-mails, surfgedrag, loginnamen, wachtwoorden, IP-adressen, tracking cookies enz. enz. Niet alleen geschreven tekst kan een persoonsgegeven zijn, ook beeld en geluid kunnen persoonsgegevens zijn.

Politiegegevens
Politiegegevens zijn persoonsgegevens die de boa op basis van de Wet politiegegevens (Wpg) in de opsporingstaak verwerkt.

Privacy by design en default
Privacy by design betekent dat er bijvoorbeeld bij het ontwerpen van een informatiesysteem of nieuw product rekening gehouden wordt met privacy. Privacy by default betekent dat standaardinstellingen zo privacyvriendelijk mogelijk zijn. Dit zijn wettelijke verplichting onder de Avg. Met andere woorden: het pro-actief borgen van gegevensbescherming in beleid, procedures en processen.

Rechten van betrokkenen
Onder de Avg hebben mensen mogelijkheden om voor zichzelf op te komen als hun persoonsgegevens worden verwerkt. Het gaat om de navolgende rechten:

- Het recht op inzage: het recht van mensen om de persoonsgegevens die de gemeente van hen verwerkt in te zien.
- Recht op rectificatie en aanvulling: het recht om de persoonsgegevens die de gemeente verwerkt te wijzigen.
- Het recht op verwijdering: het desgevraagd wissen van persoonsgegevens van betrokkene.
- Het recht op vergetelheid: het recht om 'vergeten' te worden. Dat wil zeggen dat iedere koppeling naar of kopie van de gegevens worden gewist.
- Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
- In de situatie van geautomatiseerde besluitvorming en profilering: het recht op een menselijke blik bij besluiten.
- Het recht op dataportabiliteit: het recht om persoonsgegevens over te dragen. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Het recht op duidelijke informatie over wat de gemeente met hun persoonsgegevens doet.

Verantwoordingsplicht
De Avg legt de verantwoordelijkheid bij de gemeente als organisatie om aan te tonen dat de gemeente aan de privacyregels voldoet. Verantwoordelijkheid is het vermogen om compliance met de Avg aan te tonen. Dit is dus voor verantwoordelijken en verwerkers verplicht. De verantwoording kan vormgegeven worden door het bijhouden van de verschillende registers: verwerkingsregister, datalekken, verwerkersovereenkomsten etc.

Verwerken / verwerking
Dit is in feite alles wat de gemeente doet met persoons- en politiegegevens. Het omvat de hele levenscyclus van informatie, en alles wat je doet of zou kunnen doen met deze gegevens. Bijvoorbeeld: verzamelen, vastleggen, ordenen, structureren, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, combineren, afschermen of wissen, et cetera.

Verwerker
Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt , zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Verwerkersovereenkomst
Dit is een overeenkomst tussen verantwoordelijke en verwerker, waarin de verantwoordelijkheden en afspraken over de verwerking worden vastgelegd. De overeenkomst regelt vaak algemene zaken zoals aansprakelijkheid, plus een bijlage waarin de specifieke kenmerken rondom de verwerking worden benoemd.

(Verwerkings)verantwoordelijke
Dit is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Bij de gemeente is dit, afhankelijk van de taak, het college, de burgemeerster of de gemeenteraad.

Verwerkingsregister
De gemeente is verplicht een register bij te houden van alle verwerkingen van persoonsgegevens. Dit register moet continu actueel worden gehouden. In het verwerkingsregister staan onder meer de verwerkingsdoeleinden, beschrijving van de categorieën betrokkenen en van de categorieën persoonsgegevens, de beoogde bewaartermijnen (de termijnen waarbinnen de persoonsgegevens moeten worden gewist) en een beschrijving van de wijze waarop de gegevens beveiligd zijn.

Bijlage: Beheersmaatregelen

Iedere gemeente moet volgens de IBD 100% van de criteria uit het toetsingskader naleven, tenzij zij gemotiveerd kan uitleggen dat een bepaald criterium niet van toepassing is. De thema's zijn onderverdeeld in 28 onderwerpen en 155 beheersmaatregelen. In deze bijlage bespreek ik de toetsing op de belangrijkste thema's en onderwerpen die de basis vormen voor AVG-compliance. Bij ieder thema en onderwerp benoem ik de getoetste maatregelen waaraan de gemeente volgens het IBD-toetsingskader moet voldoen, tenzij gemotiveerd uitgelegd wordt waarom een maatregel niet van toepassing is.

Dantumadiel heeft een nieuwe, eigen organisatie op moeten bouwen, en is daar in 2024 nog steeds mee bezig. Dat betekent dat ook de privacy-organisatie nog niet volledig op orde is. In dit verslag beperkt de FG-de toetsing daarom tot de thema's en onderwerpen die nodig zijn om te beoordelen of de basis op orde is. Niet alle 155 beheersmaatregelen zijn getoetst. Vanuit die basis kan dan aan verdere verbetering gewerkt worden.

De implementatie van de maatregelen wordt door middel van iconen weergegeven:

	Groei / verbetering
	Consolidatie: het gewenste niveau is bereikt, er wordt geen verdere actie tot verbetering ingezet.
	Stilstand
	Achteruitgang
	Niet getoetst/ niet van toepassing

2.1 Thema: Beleid

Het thema Beleid toetst of de organisatie processen en bijbehorende verantwoordelijkheden en risico's in kaart heeft gebracht en vastgelegd in beleidsstukken. Deze stukken moeten voor alle werknemers goed vindbaar en begrijpelijk zijn.

2.1.1 Privacybeleid

Uitleg: er is privacybeleid vastgesteld voor de gehele organisatie.

1.2.1: Het privacybeleid beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in artikel 5 lid 1 AVG zijn opgenomen.	
Toetsing: Op 29 mei 2018 heeft de gemeenteraad van Dantumadiel de Privacyverordening vastgesteld. De verordening strekt tot nadere uitwerking van de AVG. De verordening bevat bepalingen over het register van verwerkingsactiviteiten, de uitvoering van DPIA's, het behandelen van datalekken, de rechten van betrokkenen en de bevoegdheden van de FG. Op 27 maart 2018 heeft het college van b&w van Dantumadiel privacybeleid vastgesteld.	

1.2.2 Het privacybeleid beschrijft hoe de organisatie uitvoering geeft aan de verplichtingen die op de organisatie rusten op grond van privacywetgeving en materiewetgeving bij de verwerking van persoonsgegevens.	
Toetsing: Het privacybeleid beschrijft de maatregelen die getroffen zijn om persoonsgegevens rechtmatig, behoorlijk en transparant te kunnen verwerken. Deze maatregelen zijn niet of onvoldoende geïmplementeerd.	

1.2.3 Het privacybeleid beschrijft de rollen, taken en verantwoordelijkheden van de functionarissen die bij de uitvoering van het beleid zijn betrokken.	
Toetsing: Het beleid is beschreven voor de bestuurlijke samenwerking in DDFK-verband. In het beleid zijn rollen, taken en verantwoordelijkheden beschreven die in vanaf 2024 niet in de organisatie van de zelfstandige gemeente Dantumadiel bestaan of zijn toegewezen. De directie is op concernniveau verantwoordelijk voor de juiste implementatie van de informatieveiligheidsmaatregelen in de bedrijfsprocessen en in de in- en externe (informatie)systemen. De teammanagers hebben eenzelfde verantwoordelijkheid voor hun eigen teams en zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun teams (artikel 8 Organisatiebesluit Dantumadiel 2024). *Rol: Functionaris voor Gegevensbescherming (FG)*	

Het Organisatiebesluit Dantumadiel 2024 bepaalt dat er een FG is. Deze wordt via een dienstverleningsovereenkomst (hierna: dvo) afgenomen van de gemeente Noardeast-Fryslân. De taken van de FG zijn beschreven in de dvo.

Rol: Beheerder Informatieveiligheid (BIV)
In de verordening en het beleid is de rol van Beheerder Informatieveiligheid beschreven. Ieder organisatieonderdeel, afdeling of team heeft een contactpersoon die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffend organisatieonderdeel. Deze rol is niet belegd in de organisatieonderdelen van Dantumadiel.

Rol: privacy-oficer (PO)
Deze rol is niet beschreven in het privacybeleid, maar is wel een belangrijke functie in een organisatie. Waar de FG strategisch adviseur is, is de PO adviseur op tactisch niveau. De rol van de BIV is operationeel.
Dantumadiel heeft er bewust voor gekozen om geen formatie voor een privacy-officer te hebben. De taken zijn min of meer informeel belegd bij de CISO en de concerncontrollers. Dit leidt tot het risico dat noodzakelijke werkzaamheden niet, niet tijdig of niet voldoende worden opgepakt en uitgevoerd. Denk bijvoorbeeld aan het behandelen van datalekken, inzageverzoeken, opstellen en onderhouden van beleid, werkinstructies, et cetera.

1.2.5 Het privacybeleid is bekend gemaakt binnen de gehele organisatie.	
Toetsing: Er is geen specifieke vindplaats waar het vastgestelde beleid kan worden ingezien. Op het intranet (Dante) wordt de sectie ‘Weten en regelen’ ingericht. In 2025 zal het privacybeleid worden opgenomen.	

1.2.6 Het privacybeleid wordt periodiek, maar ten minste eenmaal per 36 maanden, herzien.	
Toetsing: Het privacybeleid bepaalt dat het eens per twee jaar geëvalueerd wordt en als dat nodig is (eerder) bijgesteld. Het privacybeleid is in 2018 vastgesteld en daarna niet geëvalueerd en waar nodig aangepast.	

1.2.7 Beleidsdocumenten over andere onderwerpen zijn in lijn met het privacybeleid.	
Toetsing: De maatregel is niet getoetst. Er is geen centrale vindplaats waar het vastgestelde beleid vindbaar en raadpleegbaar is.	

1.2.8 De organisatie heeft geïnventariseerd voor welke domeinen het noodzakelijk is om over domeinspecifieke uitwerkingen van het privacybeleid te beschikken om correcte omgang met persoonsgegevens binnen het desbetreffende domein te verzekeren.	
Toetsing:	

1.2.9 De organisatie heeft domeinspecifieke uitwerkingen van het privacybeleid vastgesteld voor de domeinen waarvoor dit is vastgesteld.	
Toetsing: De maatregel is niet getoetst, zie 1.2.8	

2.1.2 Verantwoordelijkheden

Uitleg: Verantwoordelijkheden voor het realiseren van de doelstellingen van het privacybeleid zijn benoemd, belegd en vastgesteld.

1.3.1 In beleid is vastgelegd dat het management verantwoordelijk is voor het realiseren van de doelstellingen van het privacybeleid van de organisatie.	
Toetsing: In het privacybeleid is een RASCI-tabel opgenomen waarin per rol de verantwoordelijkheden in beeld zijn gebracht. Het college van B&W, respectievelijk de burgemeester, is bestuurlijk verantwoordelijk is voor het naleven van de uitgangspunten en dit bij de nationale toezichthouder moet kunnen (laten) aantonen. De directie/gemeentesecretaris is ambtelijk verantwoordelijk voor risicomanagement, implementatie en naleving van de beleidsregels. Managers en teamleiders zijn verantwoordelijk voor de zorgvuldige verwerking van persoonsgegevens die binnen zijn/haar team plaatsvinden en wordt daarbij ondersteund door de Beheerder Informatieveiligheid van de afdeling/het team. In het Organisatiebesluit Dantumadiel 24 is vastgelegd dat de directie op concernniveau verantwoordelijk is voor de juiste implementatie van de informatieveiligheidsmaatregelen in de bedrijfsprocessen en in de in- en externe (informatie)systemen. De teammanagers hebben eenzelfde verantwoordelijkheid	

voor hun eigen teams en zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun teams.

2.2 Thema: Processen

Het thema Processen toetst of de organisatie alle processen waarbinnen persoonsgegevens worden verwerkt in kaart heeft gebracht. De beschrijving van deze processen wordt actueel gehouden, werkinstructies worden nageleefd en processen met een hoog risico worden getoetst op juistheid.

2.2.3 Werkprocessen

Uitleg: De organisatie heeft de werkprocessen waarin persoonsgegevens worden verwerkt in beeld en beschreven.

2.1.1 Werkprocessen waarbinnen persoonsgegevens worden verwerkt zijn eenduidig beschreven en vastgesteld.	↘
Toetsing: Werkprocessen zijn niet beschreven en vastgesteld. Binnen het sociaal domein zijn in 2024 procesverbeteringen onderzocht.	

2.2.4 Verwerkingsregister

Uitleg: De organisatie houdt een verwerkingsregister bij dat voldoet aan de bij wet gestelde eisen en houdt deze continu actueel.

2.2.1 Alle bij wet voorgeschreven onderdelen zijn in het verwerkingsregister aanwezig (artikel 30 lid 1 en 2 AVG)	↘
Toetsing: Er is geen register van verwerkingsactiviteiten.	

2.2.2 In het verwerkingsregister is voor iedere verwerking vastgelegd of de organisatie verwerkingsverantwoordelijke, verwerker of gezamenlijk verwerkingsverantwoordelijke is.]	↘
Toetsing: Er is geen register van verwerkingsactiviteiten.	

2.2.3 De organisatie heeft alle verwerkingen van persoonsgegevens correct vastgelegd in het register en het register is up-to-date.	👁
Toetsing: Er is geen register van verwerkingsactiviteiten.	

2.2.4 Het register kan desgevraagd aan de Autoriteit Persoonsgegevens worden overhandigd.	↘
Toetsing: Er is geen register van verwerkingsactiviteiten.	

2.2.5 De organisatie heeft voor iedere verwerking vastgesteld dat deze plaatsvindt in overeenstemming met de privacybeginselen. Bij een wijziging van een verwerking wordt deze beoordeling opnieuw uitgevoerd.	👁
Toetsing: Er is geen register van verwerkingsactiviteiten. Er bestaat daarom geen of onvoldoende zicht op de verwerkingen van persoonsgegevens en of deze in overeenstemming met artikel 5AVG worden verwerkt.	

2.2.6 Er is vastgelegd welke functionaris eindverantwoordelijk is voor het proces dat de volledigheid en accuraatheid van het verwerkingsregister waarborgt.	↘
Toetsing: Er is geen register van verwerkingsactiviteiten. Er is geen proces of procedure om de volledigheid en actualiteit van het register periodiek te borgen.	

2.2.7 Voor iedere verwerking is een eigenaar vastgesteld.	👁
Toetsing: Er is geen register van verwerkingsactiviteiten. Het eigenaarschap van werkprocessen en verwerkingen van persoonsgegevens is niet belegd.	

2.2.8 In een procedure is vastgelegd waar nieuwe en gewijzigde verwerkingen moeten worden gemeld teneinde deze op te nemen in het verwerkingsregister.	↘
Toetsing: Er is geen register van verwerkingsactiviteiten. Er is geen proces of procedure om de volledigheid en actualiteit van het register periodiek te borgen.	

2.2.9 In een procedure is vastgesteld met welke interval een beoordeling wordt uitgevoerd of het verwerkingsregister nog volledig en actueel is en welke functionaris hiervoor verantwoordelijk is.	↘

Toetsing: Er is geen register van verwerkingsactiviteiten. Er is geen proces of procedure om de volledigheid en actualiteit van het register periodiek te borgen.

2.2.10 De organisatie beoordeelt periodiek of het verwerkingsregister actueel en volledig is.	
Toetsing: Er is geen register van verwerkingsactiviteiten. Er is geen proces of procedure om de volledigheid en actualiteit van het register periodiek te borgen.	

2.2.5 DPIA

Uitleg: De organisatie identificeert systematisch of verwerkingen een hoog risico in kunnen houden voor de rechten en vrijheden van betrokkenen. Indien een verwerking is geïdentificeerd die een hoog risico kan opleveren, wordt een DPIA uitgevoerd die aan de eisen van de AVG voldoet. De organisatie beheert de uitkomsten van DPIA's systematisch.

2.3.1 De organisatie heeft een procedure om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijkerwijs een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.	
Toetsing: Er is geen proces of procedure om te beoordelen of een DPIA verplicht of noodzakelijk is voor een (voorgenomen) verwerking van persoonsgegevens.	

2.3.2 De organisatie heeft voor alle verwerkingen bepaald of deze een hoog risico kunnen opleveren.	
Toetsing: Er is geen register van verwerkingsactiviteiten. Er bestaat daarom geen of onvoldoende zicht op de verwerkingen van persoonsgegevens en welke risico's deze kunnen opleveren.	

2.3.3 De analyse die ten grondslag ligt aan het besluit of een verwerking al dan niet een hoog risico kan opleveren is gedocumenteerd.	
Toetsing: Er is geen proces of procedure om te beoordelen of een DPIA verplicht of noodzakelijk is voor een (voorgenomen) verwerking van persoonsgegevens.	

2.4.1 Er is een procedure vastgesteld voor het uitvoeren van DPIA's op nieuwe en sterk gewijzigde verwerkingen die mogelik een hoog privacyrisico inhouden.	

Toetsing: Er is geen proces of procedure om te beoordelen of een DPIA verplicht of noodzakelijk is voor een (voorgenomen) verwerking van persoonsgegevens.

2.4.2 Het rapport voor een DPIA is gestandaardiseerd en voldoet aan de wettelijke eisen.	
Toetsing: Er is geen proces of procedure om te beoordelen of een DPIA verplicht of noodzakelijk is voor een (voorgenomen) verwerking van persoonsgegevens.	

2.4.3 De organisatie heeft voor alle geïdentificeerde hoog-risico verwerkingen een DPIA uitgevoerd.	
Toetsing: Er is geen register van verwerkingsactiviteiten. Er bestaat daarom geen of onvoldoende zicht op de verwerkingen van persoonsgegevens en welke risicco's deze kunnen opleveren. Er is geen proces of procedure om te beoordelen of een DPIA verplicht of noodzakelijk is voor een (voorgenomen) verwerking van persoonsgegevens.	

2.4.4 Er is een procedure vastgesteld voor het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd.	
Toetsing: Er is geen proces of procedure voor het opvolgen van risico's die in een DPIA zijn geïdentificeerd.	

2.4.5 De organisatie beheert in DPIA's geïdentificeerde risico's en te implementeren maatregelen op een centrale plaats.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.4.6 De procedure voor DPIA's schrijft voor dat de FG bij het uitvoeren van een DPIA ten minste wordt geconsulteerd en dat het advies van de FG schriftelijk wordt vastgelegd.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.4.7 Voor alle uitgevoerde DPIA's is een schriftelijk advies van de FG vastgelegd.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.4.8 De procedure voor DPIA's schrijft voor dat wanneer wordt afgeweken van het advies van de FG dit schriftelijk wordt vastgelegd, en stelt eveneens vast welke functionaris beslissingsbevoegd is ten aanzien van dit besluit.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.4.9 De organisatie controleert periodiek of naar aanleiding van een DPIA te implementeren maatregelen daadwerkelijk worden geïmplementeerd en het beoogd effect bereiken.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.4.10 De organisatie controleert periodiek of er nog een actuele DPIA beschikbaar is voor alle verwerkingen met een hoog privacyrisico.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

2.3 Thema: Organisatorische inbedding

Het thema Organisatorische inbedding toetst of de organisatie een FG heeft aangesteld en of medewerkers zich voor inhoudelijke vraagstukken tot een intern privacyteam kunnen richten. Er wordt doorlopend aan bewustwording gedaan.

2.3.1 Privacyteam

Uitleg: Er is -naast de FG- ruime kennis en ervaring aanwezig over privacywetgeving.

3.1.1 Er is voldoende capaciteit van een of meer privacyspecialisten beschikbaar om het management te ondersteunen bij het realiseren van de doelstellingen van het privacybeleid.	
Toetsing: Het formatieontwerp beschrijft de functie van een CISO en een FG. De uitvoerende taken van een privacy-officer zijn toegevoegd aan functie businesscontroler. In de praktijk vervult de CISO PO-taken.	

3.1.2 Er is een functionaris verantwoordelijk voor het tijdig inschatten van de gevolgen voor de organisatie van ontwikkelingen op het gebied van privacywetgeving en jurisprudentie.	
Toetsing: [beschrijf hoe opzet, bestaan en werking van de maatregel is getoetst.	

3.2.1 De organisatie heeft een FG aangesteld.	
Toetsing: <besluit> De FG is op aangemeld bij de Autoriteit Persoonsgegevens.	

3.2.2 De FG is zodanig gepositioneerd in de organisatie dat hij als onafhankelijk toezichthouder kan functioneren.	
Toetsing: De FG is gepositioneerd onder Concern Control (Staf) en heeft daarmee rechtstreekse toegang tot het hoogste leidinggevende niveau.	

3.2.3 De FG is op basis van zijn aanstellingsbesluit verantwoordelijk voor het toezien op de naleving van de AVG en het rapporteren daarover aan het bestuursorgaan.	
Toetsing: Er is geen aanstellingsbesluit. De taken die de FG wel/niet uitvoert zijn beschreven in de dienstverleningsovereenkomst.	

3.2.4 De FG heeft op basis van zijn aanstellingsbesluit de bevoegdheid om verwerkingsactiviteiten te controleren.	
Toetsing: De maatregel is niet getoetst. Er is geen aanstellingsbesluit.	

3.2.5 De FG heeft geen taken of verplichtingen die kunnen leiden tot een belangenconflict bij de uitvoering van zijn taken als FG.	
Toetsing: In de dienstverleningsovereenkomst is opgenomen dat de FG alleen de taken zoals benoemd in de AVG en Wpg uitvoert.	

3.2.6 De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken.	
Toetsing: De maatregel is niet getoetst. Het is niet voorgekomen dat de FG dergelijke instructies heeft ontvangen.	

3.2.7 De FG heeft voldoende middelen om zijn deskundigheid op peil te houden.	
Toetsing: De maatregel is niet getoetst. In de dienstverleningsovereenkomst is opgenomen dat cursussen en dergelijke ten laste komen van de uitlenende organisatie.	

3.2.8 De FG heeft voldoende tijd en middelen ter beschikking voor het uitoefenen van zijn taken.	
Toetsing: Voor de FG-functie is 0,4 fte (14,4) uur afgenomen. Tijdens de opbouwfase van Dantumadiel kan dit wellicht onvoldoende zijn, ook gezien het gegeven dat er geen privacy-officer is en de uitvoerende taken bij businesscontrolers zijn belegd. In de praktijk voert de CISO de PO-taken uit.	

3.2.9 De FG voldoet aan de functie-eisen uit artikel 37 lid 5 AVG.	
Toetsing: De maatregel is niet getoetst. De AVG stelt dat de FG wordt aangewezen op grond van professionele kwaliteiten en deskundigheid op het gebied van wetgeving en praktijk inzake gegevensbescherming, en vermogen om de wettelijke FG-taken te vervullen.	

3.2.10 De contactgegevens van de FG zijn makkelijk vindbaar voor de betrokkenen.	
Toetsing: Intern zijn de contactgegevens van de FG op het intranet te vinden. Extern is een mailadres van de FG in de privacyverklaring op de website opgenomen.	

3.2.11 De FG wordt betrokken bij opleiding en bewustwordingsprogramma's voor personeel op het gebied van privacy.	
Toetsing: De maatregel is niet getoetst.	

2.3.2 Bewustwording

Uitleg: Er zijn voldoende middelen beschikbaar om privacybescherming te bevorderen in kennis, houding en gedrag van medewerkers in de organisatie.

3.4.1 In contracten met medewerkers en contractanten, die in aanraking komen met persoonsgegevens, worden tenminste het volgende vastgelegd: • *De verantwoordelijkheden met betrekking tot het beschermen en geheimhouden van persoonsgegevens;* • *De verplichting om persoonsgegevens uitsluitend te verwerken conform de opdrachten en instructies van de verwerkingsverantwoordelijke.*	
Toetsing: De maatregel is niet getoetst.	

3.4.2 In een procedure is vastgelegd dat medewerkers en contractanten bij indiensttreding bewust worden gemaakt van hun verantwoordelijkheden met betrekking tot het beschermen en geheimhouden van persoonsgegevens.	
Toetsing: De maatregel is niet getoetst.	

3.4.3 Alle medewerkers en contractanten hebben aantoonbaar een bewustwordingstraining gevolgd die passend is voor hun functie.	
Toetsing: Binnen ARDA kunnen onderdelen aan specifieke medewerkers aangeboden worden. Hiervan is nog geen gebruik gemaakt, alle medewerkers krijgen dezelfde onderdelen aangeboden.	

3.4.4 Er is een programma om medewerkers doorlopend bewust te maken van de risico's en randvoorwaarden bij de omgang met persoonsgegevens.	
Toetsing: In juni 2024 is Arda uitgerold. Via ARDA worden trainingen op het gebied van informatieveiligheid en gegevensbescherming aangeboden. Het gebruik van Arda kan op medewerkersniveau worden gevolgd.	

3.4.5 Periodiek wordt het bewustwordingsprogramma getoetst op effectiviteit en waar nodig bijgesteld	
Toetsing: De maatregel is niet getoetst.	

2.4 Thema: Rechten van betrokkenen

Het thema Rechten van betrokkenen toetst of de organisatie aan alle wettelijke eisen die er zijn op het gebied van rechten van betrokkenen voldoet. De organisatie is transparant over hoe en welke persoonsgegevens verwerkt worden.

2.4.1 Processen rechten van betrokkenen

Uitleg: De organisatie heeft processen ingericht om uitvoering te geven aan de rechten van de betrokkene wanneer de betrokkene een verzoek indient.

4.2.1In de interne processen voor afhandeling van verzoeken van betrokkenen is ten minste het volgende opgenomen: • *op welke wijze verzoeken kunnen worden ingediend;* • *op welke wijze de identiteit van verzoeker wordt vastgesteld;* • *wie verantwoordelijk is voor de afhandeling;* • *de toepasselijke termijnen;* • *de criteria voor het toewijzen en afwijzen van een verzoek;* • *het informeren van ontvangers over een verzoek.*	
Toetsing: Er is geen proces of richtlijn voor de behandeling van verzoeken tot uitoefening van rechten.	

4.2.2 De organisatie heeft bekendgemaakt op welke wijze en in welke gevallen een betrokkene een verzoek kan indienen tot uitoefening van zijn recht op inzage, rectificatie, wissing, beperking, overdraagbaarheid en bezwaar.	
Toetsing: In de privacyverklaring op de website van de gemeente is bekendgemaakt dat een betrokkene zijn AVG-rechten kan uitoefenen, en op welke wijzen dat kan (digitaal en schriftelijk).	

4.2.3 Verzoeken kunnen zowel schriftelijk als digitaal worden ingediend.	
Toetsing: Betrokkenen kunnen met gebruik van DigiD digitaal een verzoek indienen. In de privacyverklaring op de website van de gemeente is vermeld dat betrokkenen een dergelijk verzoek schriftelijk kunnen indienen bij de FG.	

4.2.4 Betrokkenen krijgen een ontvangstbevestiging van hun verzoek en worden op de hoogte gehouden van de status van de behandeling van het verzoek.	
Toetsing: In 2024 is één digitaal verzoek tot uitoefening van AVG-rechten ingediend. Van een digitaal verzoek dat met DigiD is ingediend verstuurd het zaaksysteem een automatische ontvangstbevestiging. Er is geen proces beschreven voor de behandeling van deze verzoeken..	

4.2.5 Medewerkers die communicatie van klanten behandelen herkennen een AVG-verzoek en weten naar wie zij deze voor verdere behandeling moeten doorsturen.	
Toetsing: Deze maatregel is niet getoetst.	

4.2.6 Een beslissing op een AVG-verzoek -een (gedeeltelijke) toe- of afwijzing- geldt als een besluit in de zin van de Algemene Wet Bestuursrecht. De organisatie stuurt een bezwaarclausule onder de beslissing mee.	
Toetsing: In 2024 is één digitaal verzoek tot uitoefening van AVG-rechten ingediend. Bij het besluit is de bezwaarclausule opgenomen. Er is geen proces beschreven voor de behandeling van deze verzoeken..	

4.2.7 Er is een procesverantwoordelijke voor de afhandeling van verzoeken.	
Toetsing: Er is geen procesverantwoordelijke aangewezen. Er is geen proces beschreven voor de behandeling van deze verzoeken.	

4.2.8 Verzoeken van betrokkenen tot uitoefening van hun rechten worden binnen de wettelijke termijn afgehandeld.	
Toetsing: In 2024 is één digitaal verzoek tot uitoefening van AVG-rechten ingediend. Het besluit is binnen de termijn genomen. Er is geen proces beschreven voor de behandeling van deze verzoeken..	

4.2.9 Wanneer een termijn voor het reageren op een verzoek van een betrokkene niet wordt gehaald, wordt dit gesignaleerd en naderhand	

geanalyseerd. Op basis van de analyse worden maatregelen getroffen om dit in de toekomst te voorkomen.	
Toetsing: In 2024 is één digitaal verzoek tot uitoefening van AVG-rechten ingediend. Het besluit is binnen de termijn genomen. Er is geen proces beschreven voor de behandeling van deze verzoeken..	

Conclusie
Er is geen proces of richtlijn beschreven voor de behandeling van verzoeken voor de uitoefening van rechten op grond van de AVG en Wpg. Wanneer een verzoek met gebruik van DigiD wordt ingediend, dan wordt in het zaaksysteem automatisch een zaak aangemaakt. Het is niet bekend of deze verzoeken als AVG- of Wpg-verzoek herkend worden wanneer deze via andere kanalen (schriftelijk, mail) binnenkomen.

2.5 Thema: Gegevensbescherming

2.5.1 Privacy-incidenten en datalekken

De organisatie detecteert en behandelt privacygerelateerde incidenten op systematische wijze.

6.5.1 De organisatie heeft een proces vastgesteld voor het detecteren en afhandelen van privacyincidenten.	
Toetsing: Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.2 Het privacyincidentenproces bepaalt: • *via welk kanaal en binnen welk tijdspad medewerkers een (vermoed) privacy-incident dienen te melden;* • *welke functionaris bepaalt of het privacyincident een inbreuk in verband met persoonsgegevens (datalek) betreft dat moet worden gemeld aan de AP en in voorkomend geval aan betrokkenen;* • *wie verantwoordelijk is voor het coördineren van de afhandeling van het privacyincident;* • *de documentatievereisten bij het afhandelen van een privacyincident.*	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.3 Het privacyincidentenproces bepaalt wie verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.4 Het privacyincidentenproces geeft een afwegingskader omtrent het al dan niet melden van een datalek aan de AP.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.5 Het privacyincidentenproces bepaalt wie verantwoordelijk is voor het melden van een datalek bij betrokkenen.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.6 Het privacyincidentenproces geeft een afwegingskader omtrent het al dan niet melden van datalekken aan betrokkenen.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.7 De organisatie heeft zowel voor interne als externe doelgroepen een meldpunt voor privacy-incidenten.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.8 Als onderdeel van het bewustwordingsprogramma worden medewerkers bekend gemaakt met hun verantwoordelijkheden ten aanzien van privacyincidenten.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.9 De organisatie is in staat om een datalek tijdig bij de AP te melden.	

Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.

6.5.10 Het SOC (Security Operations Center) heeft heldere regels over wanneer een incident als privacyincident moet worden aangemerkt en opgevolgd.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.11 Als onderdeel van het prcivacyincidentproces wordt na ieder privacyincident een evaluatie uitgevoerd om correcties en verbeteringen te identificeren.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.12 De resultaten van de evaluatie van een privacyincident worden aan het managemen gecommuniceerd.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

6.5.13 Er is een crisiscommunicatieplan voor datalekken met hoge impact.	
Toetsing: De maatregel is niet getoetst. Er is geen proces voor het afhandelen van privacyincidenten.	

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: e8760962-16d5-45f2-b53a-6a3e28e09006

Melddatum: 19 mei 2025

Meldtijdstip: 11:43

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	50820753
Naam van het bedrijf of de organisatie	Gemeente Dantumadiel
Adres	Hynsteblom 4
Postcode	9104BR
Plaats	Damwâld

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e @dantumadiel.frl
Telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Nee

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Ja
(Mogelijke) startdatum van de inbreuk	1-1-2009
4.2 Wanneer is het incident ontdekt?	19-5-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	We hebben een -mail ontvangen van Omrop Fryslân dat zij het domein dantumadiel.nl geregistreerd hebben. Op dat domein zijn 36 mails ontvangen die bedoeld waren voor de gemeente. Sommige e-mails bevatten persoonsgegevens als een BSN, NAW-gegevens, et cetera. Ook bleek een softwarepakket van de afdeling Wijkbeheer gekoppeld aan een mailadres op @dantumadiel.nl waardoor bijvoorbeeld informatie over het verlof van medewerkers werd doorgestuurd. De gemeente roept inwoners op eigen publicaties op om contact op te nemen via een mailadres op @dantumadiel.nl
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Betrokkene hebben mails met persoonsgegevens naar een mailadres op een domein dat niet in het bezit is van de gemeente.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	De gemeente Dantumadeel heeft sinds 1 januari 2009 de gemeentenaam 'verfriest' naar Dantumadiel. Het domein dantumadiel.nl bleek te zijn geregistreerd door een derde. Deze was slechts bereid de domeinregistratie over te dragen tegen een hoge vergoeding. De gemeente is daar toen niet op ingegaan. Nadien zijn voor zover bekend geen acties ondernomen om het domein te kunnen registreren. (Een medewerker van) Omrop Fryslân heeft op enig moment dit domein kunnen registreren. Na die registratie zouden daarop minstens 36 e-mails zijn ontvangen die persoonsgegevens bevatten. Op gemeentelijke publicaties (bekendmakingen en website) over grondverkopen is enkele malen een e-mailadres op het nl-domein gepubliceerd waar belangstellenden informatie op konden vragen. Zie bijvoorbeeld https://www.dantumadiel.frl/voornemen-grondverkoop-de-wylgen-feanwalden en https://www.dantumadiel.frl/sites/default/files/2025-02/gemeentepagina-19-februari-2025.pdf

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Burgerservicenummer (BSN)

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Onbekend: we gaan de ontvangen mails opvragen bij de huidige houder van het domein.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Het gaat vermoedelijk om derden (burgers) die naar het betreffende domein hebben gemaild. Door de koppeling van een softwarepakket aan een e-mailadres op dat domein zijn vermoedelijk gegevens van werknemers gestuurd.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	36

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Nog niet bekend, is afhankelijk van de inhoud van de mails. Deze vragen wij op bij de huidige houder van het domein.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Beperkt
Licht uw keuze toe:	Nog niet bekend, is afhankelijk van de inhoud van de mails. Deze vragen wij op bij de huidige houder van het domein.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nog niet bekend

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	Nog niet bekend, is afhankelijk van de inhoud van de mails. Deze vragen wij op bij de huidige houder van het domein.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Nog niet bekend

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Nog niet bekend

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	30-5-2025

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: e8760962-16d5-45f2-b53a-6a3e28e09006

Melddatum: 30 mei 2025

Meldtijdstip: 09:05

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een bestaande melding aanvullen of aanpassen
Beschikt u over het meldingsnummer van de oorspronkelijke melding?	Ja
Dit is het meldingsnummer:	e8760962-16d5-45f2-b53a-6a3e28e09006

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam	5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e @dantumadiel.frl
Telefoonnnummer	5.1.2e
2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling	Ja

3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

[✓] Aantal inbreuken in bulk

[✓] Geselecteerde toezichthouders

2. Grensoverschrijdende inbreuk

[✓] Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

[✓] Gegevens verwerkingsverantwoordelijke

[✓] Gegevens over andere organisaties

4. Tijdlijn

[✓] Tijdlijn

5. Gegevens over de inbreuk

[✓] Aard van de inbreuk

[✓] Aard van het incident

[✓] Samenvatting van het incident

6. Betrokken persoonsgegevens

[✓] Welke persoonsgegevens

[✓] Hoeveelheid persoonsgegevens

7. Getroffen personen

[✓] Groep mensen dat getroffen is door de inbreuk?

[✓] Nadere omschrijving van de groep mensen dat getroffen is door de inbreuk.

[✓] Aantal personen die door de inbreuk zijn getroffen

8. Maatregelen vooraf

[✓] Maatregelen vooraf

9. Gevolgen

[✓] Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens

[✓] Gevolgen voor de betrokkene(n) (Persoon of personen van wie gegevens zijn getroffen door de inbreuk)

10. Vervolgacties

[✓] Informeren van de betrokkene(n) (de getroffen persoon of personen)?

[✓] Maatregelen om de inbreuk aan te pakken?

1 Introductie (vervolg)

Geef het aantal inbreuken aan dat u bij de AP in bulk wilt melden:	1

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 Uw contactgegevens

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.2e
KvK-nummer	50820753
Naam van het bedrijf of de organisatie	Gemeente Dantumadiel
Adres	Hynsteblom 4
Postcode	9104BR
Plaats	Damwâld

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Gemeente

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja

Geef aan welke andere organisaties betrokken waren bij de inbreuk?

Naam	Op welke wijze betrokken	Toelichting (optioneel)
Omrop Fryslân	Journalist heeft .nl-domeinnaam van de gemeente tijdelijk gehuurd en heeft daarop e-mails met persoonsgegevens ontvangen die voor de gemeente waren bestemd.	

4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Nee
(Mogelijke) startdatum van de inbreuk	8-5-2025
(Mogelijke) einddatum van de inbreuk	18-5-2025
Wanneer heeft u het datalek voor het eerst aan de AP gemeld?	19-5-2025
4.2 Wanneer is het incident ontdekt?	19-5-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	We hebben een -mail ontvangen van een journalist van Omrop Fryslân dat zij het domein dantumadiel.nl geregistreerd hebben. Op dat domein hebben zij 36 e-mails ontvangen die bedoeld waren voor de gemeente. Sommige e-mails bevatten persoonsgegevens zoals een BSN, NAW-gegevens, et cetera. Ook bleek een softwarepakket gekoppeld aan een e-mailadres op het dantumadiel.nl-domein waar informatie over ziektemeldingen van een medewerker naar is verstuurd. In een aantal publicaties bleek de gemeente zelf een mailadres op dantumadiel.nl te hebben gecommuniceerd.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Ja

5 Gegevens over datalek

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

[✓] Overig

Namelijk:	Betrokkene hebben mails met persoonsgegevens naar een mailadres op een domein dat op dat moment niet in het bezit was van de gemeente.

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	De gemeente Dantumadiel heeft in 2009 de gemeentenaam 'verfriest' van Dantumadeel naar Dantumadiel. De domeinnaam dantumadeel.nl bleek te zijn geregistreerd door een domeinenbank. De gemeente kon deze domeinnaam kopen voor een bepaald bedrag, maar de gemeente was toen niet bereid om het gevraagde bedrag daarvoor te betalen. Nadien zijn voor zover bekend geen acties ondernomen om het domein alsnog in bezit te krijgen. Een journalist van Omrop Fryslân heeft op of rond 8 mei 2025 de domeinnaam gehuurd. Deze was voor €5 per maand te huur. Hij heeft in een tijdsbestek van tien dagnen 36 e-mails op dat domein ontvangen. (Een deel van) die e-mails bevatten persoonsgegevens. De journalist heeft bevestigd dat hij de ontvangen e-mails heeft vernietigd en de verzenders geïnformeerd dat de e-mails niet naar de gemeente waren verstuurd, maar naar de journalist. In een aantal gemeentelijke publicaties (bekendmakingen en website) is enkele malen een e-mailadres op het nl-domein gepubliceerd waar belangstellenden informatie konden vragen.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Naam

[✓] Geslacht

[✓] Burgerservicenummer (BSN)

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

[✓] Gegevens over iemands gezondheid

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	99
Geef een toelichting op bovengenoemd aantal:	Onbekend. De tijdelijke huurder van het domein heeft aangegeven dat hij de ontvangen mails heeft verwijderd. De betrokkenen en de inhoud van de ontvangen mails is daarom niet meer te achterhalen.

7 Betrokkenen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Klanten (huidig en potentieel)

[✓] Minderjarigen

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	De tijdelijke huurder van het domein heeft aangegeven dat hij de ontvangen mails heeft verwijderd. De betrokkenen en de inhoud van de

ontvangen mails is daarom niet meer te achterhalen. Volgens screenshots van een aantal ontvangen e-mails gaat het in ieder geval om: - werknemers: in een softwarepakker was een e-mailadres voor taaknotificaties op het .nl-domein gezet. Er zijn in ieder geval een mail verstuurd over een medewerker die zich meermalen ziek heeft gemeld, en een mail om een declaratie te fiatteren; - klanten (burger/inwoner): een vraag aan het	gebiedsteam (sociaal domein) over opvolging van zaken die tijdens een huisbezoek zijn besproken; - ondernemer: een aangifte toeristenbelasting per mail ingediend. Het aangifteformulier bevat persoonsgegevens van de personen die in 2024 op de locatie van de ondernemer hebben verbleven; - zorgverlener: verzoek om nadere berichtgeving over jeugdzorg met vermelding van het BSN van de betrokkene, voor zover bekend geen andere persoonsgegevens in dat bericht.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	99

8 Maatregelen

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Onbekend. De tijdelijke huurder van het domein heeft aangegeven dat hij de ontvangen mails heeft

verwijderd. De betrokkenen en de inhoud van de	ontvangen mails is daarom niet meer te achterhalen.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Verwaarloosbaar
Licht uw keuze toe:	De tijdelijke huurder van het domein heeft aangegeven dat hij de ontvangen mails heeft verwijderd. De betrokkenen en de inhoud van de ontvangen mails is daarom niet meer te achterhalen. De tijdelijke huurder heeft de verzenders van de mail geïnformeerd dat de verzonden mail niet door de gemeente, maar door de journalist is ontvangen.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Nee
Gaat u de inbreuk nog melden aan de betrokkene(n)?	Nee

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	De tijdelijke huurder van het domein heeft aangegeven dat hij de ontvangen mails heeft verwijderd. De betrokkenen en de inhoud van de ontvangen mails is daarom niet meer te achterhalen. De tijdelijke huurder heeft de verzenders van de mail geïnformeerd dat de verzonden mail niet door de gemeente, maar door de journalist is ontvangen.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	1. De gemeente heeft het domein dantumadiel.nl op 20 mei 2025 aangekocht. Een bezoek aan dantumadiel.nl wordt sinds die datum doorgeleid naar de officiële gemeentelijke website dantumadiel.frl. 2. Onze functioneel beheerder en de leverancier van het HRM-pakket heeft onderzocht waar in het pakket mailadressen van @dantumadiel.nl voorkomen en deze aangepast. 3. Email die naar een mailadres @dantumadiel.nl wordt gestuurd zal naar het @dantumadiel.frl worden doorgestuurd. Wij zijn hiervoor afhankelijk van onze ICT-partner Shared Service Center Leeuwarden. 4. Voor publicaties op de gemeentelijke website wordt het vier-ogenprincipe toegepast.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Email die naar een mailadres @dantumadiel.nl wordt gestuurd zal naar het @dantumadiel.frl worden doorgestuurd. Wij zijn hiervoor afhankelijk van onze ICT-partner Shared Service Center Leeuwarden. Voor publicaties op de gemeentelijke website wordt het vier-ogenprincipe toegepast.

11 Verzenden

Is dit een voorlopige of een definitieve melding?	Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP

Datum	Prio	TopDesk	Inbreuk: gegevens zijn (onbevoegd)	Beschrijving van de inbreuk	In/extern	(Mogelijke) gevolgen voor betrokkenen Getroffen maatregelen	Melding aan AP?	Datum melding AP	Melding betrokkene(n)	Datum melding	Tekst kennisgeving aan betrokkene(n)	Veran tw	Team	Categorie
11-01-2024	Laag		Gelezen (vertrouwelijkheid)	Op de website van Dantumadiel stond een telefoonnummer van Noardeast-Fryslân voor het gebiedsteam. Een inwoner heeft dat nummer gebeld en haar hulpvraag besproken met een medewerker van Noardeast-Fryslân. Daarbij is er door een medewerker van Noardeast-Fr	Extern	Telefoonnummers op de website worden zsm aangepast. KCC-Noardeast is geïnformeerd dat er nog NF-telefoonnummers op de website van Dantumadiel worden vermeld.	Nee	Geen melding aangezien er geen gevoelige data met personen is gedeeld die daar een mogelijk kwaad mee kunnen verrichten. En het aantal betrokken bewoners is laag, en er is niet informatie met een derde gedeeld waarvoor geen grondslag is.	Nee, gevolgen onwaarschijnlijk	nvt	nvt	College	Dienstverlening	Overig
21-03-2024	Laag		Gelezen (vertrouwelijkheid)	Er is in de de periode van 1-1-2024 tot 21-3- 2024 gebruik gemaakt van de applicatie omgeving van Dantumadiel [redacted] door 3 onbevoegde mensen. Dit zijn medewerkers van NO geweest.	Intern	Ja alle rechten zijn ingetrokken voor deze personen en daarmee is er geen toegang meer mogelijk	Nee	Geen melding aangezien er geen data met externe personen is gedeeld die een inbreuk kunnen hebben op iemands prive situatie. Er treft niemand persoonlijk leed	Nee, getroffen maatregelen bieden voldoende bescherming			College	Dienstverlening	Overig
03-07-2024			Gelezen (vertrouwelijkheid)	Een medewerker van het KCC heeft een mail van een inwoner van de gemeente Dantumadiel verzonden naar [redacted]@leeuwarden verzonden ipv @ dantumadiel. Klant heeft een klacht gedaan [redacted] eeft klant gebeld en daarmee is de zaak afgedaan en heeft de kla	Extern	buiten onze organisatie maar binnen de samenwerkingsovereenkomst	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, getroffen maatregelen bieden voldoende bescherming			College	Dienstverlening	E-mail aan verkeerde ontvanger(s)
15-07-2024			Gelezen (vertrouwelijkheid)	Een medewerker van het KCC heeft een mail van een inwoner van de gemeente Dantumadiel verzonden naar [redacted]@leeuwarden verzonden ipv @ dantumadiel	Extern	buiten onze organisatie maar binnen de samenwerkingsovereenkomst	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, getroffen maatregelen bieden voldoende bescherming			College	Dienstverlening	E-mail aan verkeerde ontvanger(s)
17-07-2024	Midden		Gelezen (vertrouwelijkheid)	In het beheersysteem van [redacted]s de data van burgers van Dantumadiel te raadplegen door NO medewerkers	Intern	Er is een melding bij [redacted]gemaakt om de data niet meer zichtbaar te houden voor NO	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, gevolgen onwaarschijnlijk			College	Sociaal Domein	Pgg van verkeerde klant getoond in portaal
15-09-2024	Laag		Geen / overig	Medewerkers van Sociaal domein heeft een dubieus telefoontje gahd. Niet opgenomem. Voicemail bericht deed het verzoek om terug te bellen ivm een noodgeval. Alles in het engels	Intern	nummer geblokkeerd en geen schade aangericht	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde					Sociaal Domein	Overig
24-09-2024	Hoog		Gelezen (vertrouwelijkheid)	Op de R schijf van Dantumadiel staan stukken van de Jeugd omgeving van NO	In- en extern	Er is een melding bij het het SSC gedaan met het verzoek om de bestanden over te zetten naar NO en de juiste bestanden van Dantumadiel op deze locatie te plaatsen	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, gevolgen onwaarschijnlijk			College		Netwerkmappen te breed toegankelijk
07-10-2024		C2410-1470		Melder heeft een bericht verstuurd aan iemand buiten de organisatie ipv aan een collega (beiden met dezelfde voornaam). Er stond geen vertrouwelijke informatie in het bericht, behalve twee e-mailadressen van collega's en van de melder.	Extern								Openbare Werken	E-mail aan verkeerde ontvanger(s)
22-10-2024	Laag		Gelezen (vertrouwelijkheid)	Er zijn met [redacted]gegevens van een dossier verzonden met daarbij stukken van een derde burger. Stukken zijn direct teruggehaald met cryptshar	Intern	Medewerker heeft de stukken terugehaald en daarmee is schade uitgesloten	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, getroffen maatregelen bieden voldoende bescherming			College	Sociaal Domein	Overig
10-12-2024		C2412-2715		In een Excelbestand is een tabblad met namen van stembureauleden met de vergoeding die zij hebben gekregen meegezonden naar een medewerker van de VNG.	Extern	Ontvanger is verzocht om het ontvangen mail en bestand te vernietigen. Nieuwe mail gestuurd zonder deze informatie.	Nee					College		Pgg per ongeluk gepubliceerd
07-01-2025		C2501-1036												
		C2501-3527												
15-01-2025		C2501-3539	Gelezen (vertrouwelijkheid)	Melder heeft een verkeerde ontvangstebevestiging naar een bewoner verstuurd. Hierin staan gegevens die niet voor de persoon zijn (naam en adres)	Extern							College	Sociaal Domein	Brief verstuurd aan de verkeerde ontvanger(s)
26-03-2025				Zie NF-call C2503-7435								College	NF (uit DVO)	
01-04-2025	Laag	C2504-0405	Gelezen (vertrouwelijkheid)	Door het versturen van een brief (via mail) naar de gemeente Waadhoeke ipv een contactpersoon van brandweer Fryslân. Het incident ontdekt doordat een collega van Waadhoeke de melder attendeerde	Extern	Medewerker Waadhoeke heeft de mail verwijderd	Nee	Geen melding aangezien de data gedeeld is met een partner gemeente en niet met een derde. Daarnaast is er geen persoonlijk leed aan de orde	Nee, gevolgen onwaarschijnlijk			College	Omgeving en Economie	E-mail aan verkeerde ontvanger(s)
19-05-2025	Hoog	C2505 3539	Gelezen (vertrouwelijkheid)	Mail Omrop Fryslân: Uit onze analyse blijkt dat de gemeente Dantumadiel het domein dantumadiel.nl niet heeft geregistreerd, terwijl dit adres wel in officiële gemeentelijke publicaties is gebruikt.	Extern	De gevolgen zijn dat er gevoelige data in het bezit is gekomen van de Omrop. Zij hebben de data verwijderd. En de gemeente Dantumadiel heeft het domein .nl gekocht	Ja	Er is een melding gedaan omdat er gevoelige data buigten de organisatie onterecht is ontvangen	Ja, datalek vormt waarschijnlijk een (hoog) risico	19-05-2025	Melding gedaan op 19 mei en inmiddels ook afgesloten.	College	Dienstverlening	Overig
20-05-2025	Laag	C2505 4106	Gelezen (vertrouwelijkheid)	Een commissielid bezwaarschriften heeft de brief gericht aan een kantoor ontvangen. Het is aangetekend verzonden, dus de bewijzen van het het anagetekend verzenden worden achterhaald	Extern		Nee	Er is geen melding gemaakt ook mede omdat het 1 enkele actie betreft en niet meerdere inwoners hiermee geraakt zijn.	Nee, gevolgen onwaarschijnlijk		nvt	College	Dienstverlening	Brief verstuurd aan de verkeerde ontvanger(s)

Categorie	2017	2018	2019	2021	2022	2023	2024	2025
E-mail aan verkeerde ontvanger(s)							3	-
E-mail met ontvangers niet in de bcc							-	-
Brief verstuurd aan de verkeerde ontvanger(s)							-	-
Brief geopend retour ontvangen							-	-
Brief of postpakket kwijtgeraakt							-	-
Autorisatie(s) verkeerd ingesteld							-	-
Netwerkmappen te breed toegankelijk							1	-
Apparaat of doc's kwijtgeraakt of gestolen							-	-
Pgg per ongeluk gepubliceerd							1	-
Phishing							-	-
Ransomware							-	-
Ander type hacking en/of malware							-	-
Raadplegen van pgg zonder legitiem doel							-	-
Pgg van verkeerde klant getoond in portaal							1	-
Pgg toegevoegd aan het verkeerde dossier							-	-
Pgg bij oud papier gezet							-	-
Pgg door storing (tijdelijk) niet beschikbaar							-	-
Overig							4	-
	0	0	0	0	0	0	10	0

Afdeling/team	Inbreuk	Melding aan AP?	Melden betrokkene(n)	Verantwoordelijke	Gegevens zijn	Aantal betrokkenen	Gevolgen	Categorie
Advies & Ondersteuning	Ontvreemd	Ja	Ja, datalek vormt waarschijnlijk een (hoog) risico	Burgemeester		Enkel (1)		E-mail aan verkeerde ontvanger(s)
Dienstverlening	Gekopieerd	Ja, voorlopig	Nee, getroffen maatregelen bieden voldoende bescherming	College		Aantal (<10)		E-mail met ontvangers niet in de bcc
Omgeving en Economie	Gelezen (vertrouwelijkheid)	Nee	Nee, gevolgen onwaarschijnlijk	Gemeenteraad		Tientallen (<100)		Brief verstuurd aan de verkeerde ontvanger(s)
Openbare Werken	Veranderd (integriteit)	Nee, voorlopig ingetrokken	Nee, zwaarwegende redenen	Anders		Honderden (<1.000)		Brief geopend retour ontvangen
Sociaal Domein	Verwijderd of vernietigd (beschikbaar)					Duizenden (<10.000)		Brief of postpakket kwijtgeraakt
NF (uit DVO)	Nog niet bekend					Allen		Autorisatie(s) verkeerd ingesteld
	Geen / overig							Netwerkmappen te breed toegankelijk
								Apparaat of doc's kwijtgeraakt of gestolen
								Pgg per ongeluk gepubliceerd
								Phishing
								Ransomware
								Ander type hacking en/of malware
								Raadplegen van pgg zonder legitiem doel
								Pgg van verkeerde klant getoond in portaal
								Pgg toegevoegd aan het verkeerde dossier
								Pgg bij oud papier gezet
								Pgg door storing (tijdelijk) niet beschikbaar
								Overig