JAARRAPPORTAGE BESCHERMING PERSOONSGEGEVENS

GEMEENTE LELYSTAD 2024

Functionaris Gegevensbescherming (FG)

Pieter Poelstra

02-04-2025

Inhoudsopgave

Inleiding

De gemeente Lelystad dient zorgvuldig om te gaan met persoonsgegevens. Onze gemeente verwerkt immers bij de uitoefening van haar taken veel informatie. Niet alleen persoonlijke informatie van eigen inwoners, maar ook van andere burgers, medewerkers, externen en zakenrelaties. In de AVG (Algemene Verordening Gegevensbescherming) wordt het wettelijk kader beschreven voor het verwerken van persoonsgegevens. Zo dient de gemeente inzichtelijk te hebben welke persoonsgegevens zij verwerkt en voor welk doel. Persoonsgegevens mogen alleen worden verwerkt wanneer dit in overeenstemming is met het doel waarvoor zij zijn verzameld en gegevens mogen niet langer bewaard worden dan noodzakelijk. Bovendien moet de gemeente passende technische en organisatorische beveiligingsmaatregelen treffen om onrechtmatige toegang tot deze persoonsgegevens tegen te gaan waarmee onrechtmatig gebruik van deze persoonsgegevens voorkomen wordt.

Onder de verantwoordelijkheid van de bestuursorganen van de gemeente Lelystad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om persoonsgegevens zoals van eigen inwoners, inwoners van andere gemeenten, medewerkers en externen. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast dient de gemeente Lelystad te beschikken over een interne toezichthouder: de Functionaris voor de Gegevensbescherming (FG). De bestuursorganen van de gemeente Lelystad alsook de lokale rekenkamer hebben Pieter Poelstra aangesteld als FG[1].

De FG ziet erop toe, vanuit zijn onafhankelijke toezichthoudende rol, dat de AVG intern wordt nageleefd. De FG dient tijdig en naar behoren te worden betrokken bij alle gelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast dient de FG ondersteund te worden door hem toegang te verschaffen tot persoonsgegevens en verwerkingen daarvan en hem de benodigde middelen ter beschikking te stellen voor het vervullen van de taak en het in standhouden van zijn deskundigheid.

De FG brengt jaarlijks een verslag uit aan de verwerkingsverantwoordelijken van zijn werkzaamheden en bevindingen en doet hij naar aanleiding daarvan aanbevelingen. Deze jaarrapportage is bedoeld voor de burgemeester en het college van B&W. De gemeenteraad zal als zelfstandig verwerkingsverantwoordelijke en als controlerend orgaan van het college van B&W eveneens dit verslag ontvangen.
Deze jaarrapportage is gebaseerd op een stramien zoals dat door de VNG ter beschikking is gesteld.

[1] Hiermee worden de drie bestuursorganen van de gemeente bedoeld: de burgemeester, het college van burgemeester en wethouders en de gemeenteraad.

Samenvatting

De gemeente Lelystad heeft vastgesteld privacybeleid op basis van de AVG (Algemene Verordening Gegevensbescherming) dat dient als kader voor de bescherming van persoonsgegevens.
Aanvullend conformeert de gemeente zich aan de BIO (Baseline Informatiebeveiliging Overheid), een voorname voorwaarde voor de bescherming van deze gegevens.
Nauwe samenwerking met leden van de CIO-Office zorgt er voor dat nieuwe projecten, applicaties en aanbestedingen in een vroegtijdig stadium over de privacy-component geadviseerd worden.
Externe partijen worden voorafgaand aan de samenwerking beoordeeld op hun omgang met persoonsgegevens; indien nodig worden verwerkersovereenkomsten getoetst en afgesloten.
Ook in 2024 zijn er zeer veel adviezen op grond van de AVG gegeven. De applicatie die veilig mailen bevordert, is verder verfijnd in de toepassing. De kans op een verkeerd gestuurde mail, niet zelden een oorzaak van een datalek, wordt hiermee verkleind. In 2024 liep het contract af met ZIVVER. Mede gelet op de gebruikerservaringen is gekozen voor Bastion 365 dat inmiddels is uitgerold in de organisatie.
De datalekken die in 2024 zijn opgetreden zijn conform procedure afgehandeld en waar nodig zijn er verbeteringen in het proces doorgevoerd.
Medewerkers zijn meer en meer hybride gaan werken. Daarom is in de bewustwording over 'Veilig werken met informatie' de nadruk gelegd om ook in de thuissituatie de richtlijnen na te leven.
Interne controles en audits uitvoeren zijn een vast onderdeel van de werkzaamheden van de FG (Functionaris Gegevensbescherming), de onafhankelijke toezichthouder op het gebied van persoonsgegevens. Daarnaast is besloten om de e-learning "AVG voor gemeenten" verplicht te stellen voor elke medewerker van de gemeente Lelystad.
Ook in 2025 zullen weer interne controles en audits uitgevoerd worden. De nieuwe actiepunten die dit gaat opleveren, zullen op opvolging gemonitord worden.

Deel 1. Terugblik op 2024

In dit deel van de rapportage zal worden teruggeblikt op hetgeen de gemeente in 2024 heeft bereikt en welke werkzaamheden zijn verricht.

1. Het privacybeleid

Het privacybeleid is een kader waarin de gemeente Lelystad aangeeft aan welke principes zij zich houdt bij de verwerking van persoonsgegevens. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de relevante wet- en regelgeving.

De gemeente Lelystad heeft het privacybeleid en –reglement (inclusief taken en bevoegdheden van de FG) in maart 2018 vastgesteld. Ook is er een Privacy Statement op de website www.lelystad.nl geplaatst. Hier staat in begrijpelijke bewoordingen de bescherming van persoonsgegevens uitgelegd. En de rechten die betrokkenen hebben, zoals het recht op inzage in hun persoonsgegevens. Er is een voorbeeldbrief opgenomen op die website die de drempel verlaagt om zo'n verzoek in te dienen. Het beleid zal in ultimo 2024 een 'opfrisser' ondergaan en worden aangeboden aan directie en College. Dit zal in het voorjaar van 2025 zijn.

2. Processen

De verwerkingen van persoonsgegevens van de gemeente Lelystad dienen te voldoen aan de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de volgende beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. Daarnaast voert de gemeente in bepaalde gevallen een gegevensbeschermingseffectbeoordeling (DPIA[2]) uit.
In bijlage 1 is een overzicht opgenomen van de uitgevoerde DPIA's en privacyscans in 2024.

Hoewel de FG omwille van zijn onafhankelijke rol geen deel uitmaakt van de CIO-Office (Chief Information Officer), werkt hij wel degelijk nauw samen met de CIO-Office en informatiemanagers. Hierdoor wordt de FG in een vroegtijdig stadium betrokken bij nieuwe initiatieven die een privacy-component hebben. De FG toetst deze initiatieven op de in de 1e alinea genoemde beginselen. De bescherming van persoonsgegevens is zodoende één van de leidende principes van "Lelystad Digitaal 2025", één van de producten van de CIO-Office. En vindt ook zijn plek is de doorstart van dit programma dat "Waardevolle Informatievoorziening" heet. Ook heeft de FG vrijwel dagelijks contact met de CISO (Chief Information Security Officer) over de stand van zaken en trends op het gebied van informatiebeveiliging. Dit onderwerp is uiteraard een noodzakelijke voorwaarde wanneer het aankomt op bescherming van persoonsgegevens.

3. Organisatorische inbedding

De FG en de Privacy Officer (PO) zijn de eerste aanspreekpunten als het aankomt op 'privacy'.
De PO adviseert op casusniveau aan medewerkers. De FG is eveneens adviseur en is daarnaast toezichthouder en verricht audits.
De werkzaamheden vallen grofweg uiteen in instrueren, adviseren en controleren.

[2] De gegevensbeschermingseffectbeoordeling wordt ook wel afgekort tot DPIA naar de Engelse term Data Protection Impact Assessment.

Instrueren
Sinds 2019 zijn door FG en PO tientallen presentaties aan teams gehouden over de (invoering van) AVG en de gevolgen daarvan voor het betreffende team. Deze presentaties zijn in 2024 op verzoek herhaald, ook vanwege het personeelsverloop binnen teams en nieuwe medewerkers binnen de gemeente. Deze presentaties worden tegenwoordig tezamen met de CISO en ISO gedaan.
Immers: voor een goede en juiste uitvoering van de AVG is het van belang dat elke medewerker binnen de organisatie op de hoogte is van de beginselen van de AVG en het belang van bescherming van persoonsgegevens.
Daarnaast heeft de PO het veilig mailen instrument 'Bastion365' in 2024 verder verfijnd door maatwerk en instructies te geven. Dit instrument is aangegrepen om andermaal het belang van zorgvuldig omgaan met persoonsgegevens te benadrukken. Er is besloten om met Bastion 365 verder te gaan (in plaats van ZIVVER) omdat deze toepassing minder foutmeldingen voor de gebruiker oplevert in de Microsoft mailomgeving.
Standaard wordt een afspraak gemaakt met nieuwe teamleiders en directieleden om hun mee te nemen in hun rol en verantwoordelijkheid betreffende de bescherming van persoonsgegevens. Vaak vloeit daar uit uitnodiging voor een teampresentatie uit voort.

Adviseren
Er zijn zeer veel adviezen gegeven over de meest uiteenlopende werkterreinen aan medewerkers die vragen hebben over de toepassing van de AVG. Meestal wordt een voorgestelde werkwijze ter toetsing voorgelegd. Soms wordt om advies gevraagd hoe het beste een proces ingericht kan worden gelet op de AVG. Inmiddels kan gesteld worden dat de medewerker het 'loket privacy' dat bemand wordt door de FG en PO goed weet te vinden. De eerder genoemde samenwerking met de CIO-Office, CISO en ISO is hier mede debet aan.

Controleren
Dit onderdeel is voor rekening van de FG die hiermee onder meer zijn toezichthoudende rol mee invult. Aanleiding kan zijn een datalek, ENSIA, periodieke beveiligingsrondes en audits.
Bij punt 8 zijn bevindingen vanuit deze controles opgenomen.

Organisatorische inbedding betekent tevens het toewijzen van taken, verantwoordelijkheden en bevoegdheden en bewustzijn creëren. In het privacybeleid zijn daarom de verantwoordelijkheden en taken toegewezen. Uitgangspunt is dat eenieder die werkt met persoonsgegevens, de beginselen van de AVG weet toe te toepassen.
Tot slot: op grond van artikel 38 lid 3 van de AVG mag de FG geen instructies ontvangen met betrekking tot de uitvoering van zijn taken. In 2024 heeft de FG zonder interventies zijn werk kunnen doen en ondervindt hij geen belemmeringen in de uitvoering van zijn werk.

4. Rechten van betrokkenen

In het Privacy Statement staat verwoord hoe de gemeente omgaat met persoonsgegevens. Ook is daar het privacybeleid en –reglement opgenomen. Het stelt betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens. Bijvoorbeeld het recht op inzage. Hier is in 2024 beperkt gebruik van gemaakt.
In bijlage 2 is een overzicht opgenomen van het aantal verzoeken van betrokkenen in het jaar 2024.

5. Samenwerking

De gemeente Lelystad werkt op meerdere beleidsterreinen, in verschillende bedrijfsfuncties, in diverse

rollen en hoedanigheden samen met (mede) overheden en private organisaties. In bepaalde gevallen zal er sprake zijn van een verwerking van persoonsgegevens tussen partijen: ontvangen van persoonsgegevens, verzenden van persoonsgegevens, maar ook het opslaan van en inzage hebben in persoonsgegevens valt onder dit begrip. Deze verwerkingen dienen dan ook te voldoen aan de AVG. De gemeente Lelystad heeft op grote schaal afspraken gemaakt met deze externe partijen.
In een zogenaamde verwerkersovereenkomst zijn deze afspraken vastgelegd. De FG houdt het register bij waarin de verwerkersovereenkomsten staan. De gemeente Lelystad heeft als uitgangspunt dat de standaard verwerkersovereenkomst van de VNG leidend is. Van deze standaard is in 2021 een nieuwe versie van de hand van de VNG verschenen die vanaf dat moment ook meteen door de gemeente Lelystad is toegepast. De betrokken teams worden van advies voorzien mocht dat nodig zijn. Bijvoorbeeld als een externe partij wil onderhandelen over de inhoud van de verwerkersovereenkomst. Het register bevat inmiddels bijna 130 verwerkersovereenkomsten.

6. Beveiliging

Vanuit het algemene behoorlijkheidsbeginsel, het integriteitsbeginsel en het vertrouwelijkheidsbeginsel is het essentieel dat de gemeente Lelystad passende technische en organisatorische maatregelen neemt ter beveiliging van persoonsgegevens. Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten – waaronder inbreuken – op de beveiliging onder omstandigheden gemeld dienen te worden aan de AP en/of de betrokkene(n).
De datalekken zijn allen afgehandeld conform procedure. De FG is hierbij de spin in het web. Hij onderzoekt bijvoorbeeld of het datalek gemeld moet worden aan betrokkenen en de AP, of de beveiligingsmaatregelen moeten worden aangepast en of een eventuele aanpassing van een beveiligingsmaatregel heeft voldaan. Alle datalekken worden conform procedure gemeld aan de gemeentesecretaris en de betreffende wethouder(s).
In bijlage 3 is een overzicht opgenomen van het aantal datalekken in 2024.
De gemeente conformeert zich bovendien aan de BIO (Baseline Informatiebeveiliging Overheid) waarover het zich in de ENSIA-systematiek (Eenduidige Normatiek Single Information Audit) jaarlijks verantwoordt aan gemeenteraad en de nationale toezichthouder. De CISO van de gemeente Lelystad neemt dit onderdeel voor zijn rekening.

7. Verantwoording

De AVG legt de verantwoordelijkheid bij de organisatie zelf om aantoonbaar te maken dat deze voldoet aan de privacyregels. Door te voldoen aan de verantwoordingsplicht levert de organisatie een belangrijke bijdrage aan de bescherming persoonsgegevens. De verplichte maatregelen van de AVG waarvoor een verantwoordingsplicht geldt (en waaraan de gemeente Lelystad voldoet) zijn:

- Register van verwerkingsactiviteiten opstellen en bijhouden
- DPIA’s uitvoeren (zie punt 2 op pagina 5)
- Register bijhouden van datalekken
- Aantonen dat betrokkene toestemming geeft voor een verwerking wanneer dat noodzakelijk is. Omdat de gemeente vanuit haar wettelijke en publieke taak veelal geen toestemming hoeft te vragen, is dit onderwerp beperkt tot bijvoorbeeld cookies op de website en nieuwsbrieven.
- Aanstellen van een FG. De AP heeft hier op gecontroleerd.

Een manier om de verantwoording vorm te geven en daarmee ook transparantie te bieden is deze jaarrapportage.

8. Conclusie

Vanaf 2018 heeft de gemeente Lelystad heel wat werk verzet om de AVG te implementeren in de organisatie, de systemen en de processen. Een aantal maatregelen waren zeer effectief, zoals het

creëren van bewustzijn (dat onder meer blijkt uit het grote aantal adviesvragen naar aanleiding van de bewustwordingssessies) en het adviseren op casusniveau. Ook zijn er vele verwerkersovereenkomsten afgesloten met externen die met persoonsgegevens werken waar de gemeente Lelystad verantwoordelijk voor blijft. Het zorgt ervoor dat deze partijen zich bewust zijn van hun handelen met betrekking tot deze persoonsgegevens. Ook zijn er organisatiebreed veel persoonsgegevens “opgeruimd” op basis van de bewaartermijnen en is de toegang in bepaalde gevallen beperkt tot de medewerkers die er ook echt mee moeten werken.
Maar er zijn ook aandachtspunten voor de organisatie waarin het nog kan groeien. In onderstaande tabel zijn de voornaamste acties benoemd die het omgaan met persoonsgegevens naar een nog hoger plan te tillen. In aanvulling uiteraard op het instrueren en adviseren zoals in punt 3 behandeld is.

Thema	**Betreft**	**Actie**	**Actuele status (april 2025)**
Sociaal Domein	i-Samenleving	Ist en Soll i-SL: trek een vergelijk tussen wat in de aanbesteding staat over Informatiebeveiliging en Privacy en wat er gerealiseerd is. Maak hierbij tevens gebruik van het adviesrapport van FG en CISO dat begin 2024 is opgesteld t.b.v. de stuurgroep i-SL. Advies is te onderzoeken om logging-controle (2e lijns controle) intern te beleggen bij IC Sociaal Domein	Van het totale project wordt momenteel aan de hand van het Programma van Eisen een lijst met openstaande punten gemaakt en in gesprek gebracht bij de leverancier
		Opruimen gegevens conform opschoonplan	Vernietigingskader is in december 2024 in het DT Sociaal Domein goedgekeurd. 2e kwartaal 2025 is de planning dat restant opgeschoond is.
		Kwalificatie “Fraude” gekoppeld aan een persoon (Participatiewet) is sinds een rechterlijke uitspraak niet toegestaan, staat echter wél frequent in CiVision. Afdwingen	Geen opvolging tot op heden, ondanks herhaalde reclamatie.

		bij leverancier dat dit wordt aangepast. 'Fraude' is nieuwe struikelterm	
Stadstoezicht	Toezicht en opsporing meldingen staan in 1 overzicht, dient gescheiden te zijn (AVG / Wpg)	Aparte overzichten genereren	Nog niet gereed, gesprekken intern met leverancier lopen nog.
GUUS (financieel system)	* Procedure opstellen en rapporteren gebruikerstoegang en review accounts (incl hoge rechten accounts) * Controle medewerker uit dienst Deze punten zijn ook opgenomen in de management letter van de accountant.	Opvolgen bevindingen	Follow audit up volgt in 2025
Fysieke controle	In mei 2024 is tezamen met de CISO en ISO een beveiligingsronde gedaan in de avonduren. Er is gecontroleerd of documenten/dossiers conform beleid zijn opgeborgen.	Dossiers/documenten met persoonsgegevens die niet waren opgeborgen zijn gemeld aan de betreffende teamleider die het vervolgens bespreekbaar heeft gemaakt in het team.	Follow audit up volgt in 2025. Op verzoek wordt dit ook op domein niveau uitgevoerd.

Onderdelen die in 2024 succesvol zijn afgerond nadat ze eerder op bovenstaande actielijst stonden, waren *onder meer*:

- Wet politiegegevens (Wpg): procedures Sociale Recherche zijn beschreven
- Sociaal Domein en Vergunningen: concreet opschoonplan in samenspraak met Informatiebeheer
- GUUS: afsluiten openstaande accounts medewerkers uit dienst
- Aanpassen vertrouwelijkheden in MyCorsa naar aanleiding van een interne controle
- Documenten/dossiers achter slot en grendel naar aanleiding van de fysieke controle

Deel 2. Vooruitkijken naar 2025

Gegevensbescherming onderdeel laten worden van de organisatie, en daarmee aantoonbaar voldoen aan de relevante wet- en regelgeving, is geen afvinklijst maar een continu proces. Het vraagt om structurele borging van dit onderwerp. Waar het jaar 2018 in het teken stond van voorbereiden op de AVG en het nemen van de eerste hobbels om uiteindelijk aantoonbaar te kunnen voldoen aan deze wet, stond 2019 in het teken staan van het continueren en verstevigen van dit proces. En het uitvoeren van audits om te toetsen of de regels worden nageleefd. In 2025 zal deze lijn worden doorgetrokken. Daarnaast zal ook aan bewustwording blijvend aandacht geschonken worden en zullen er adviezen/richtlijnen gegeven worden op casus-niveau. In 2025 worden de opbrengsten vanuit wordt de Cybersecurity Cultuurscan uitgerold. Met behulp van een vragenlijst wordt is een beeld gevormd van hoe veilig werken met informatie binnen onze organisatie gaat. En waar in de organisatie welke bijsturing nodig is. Hiermee wordt de cyclus instrueren, adviseren en controleren blijvend doorlopen.

1. Het privacybeleid

Actie: het beleid zal een opfrisbeurt ondergaan en op onderdelen een update ondergaan. Er zullen geen grote wijzigingen in het beleid hoeven plaatsvinden. Het nieuwe beleid en bijbehorende reglement zal in 2025 worden vastgesteld.

2. Processen

Naast de actiepunten zoals benoemd bij punt 8 van Deel 1 zullen de speerpunten zijn:

- Audits: GUUS (financieel systeem), Power BI, CLO, Djuma, de IT-beheeromgeving (Windows) en op fysieke dossiers (gemeentebreed).

  Naast de audits die al vanuit ENSIA worden uitgevoerd en die ook privacyaspecten in zich hebben zoals BRP (Basis Registratie Personen), DigiD, SuwiNet (Structuur Uitvoering Werk en Inkomen).

  Ook zal naar aanleiding van de Wpg een audit worden gedaan bij de teams die op basis van deze wetgeving met persoonsgegevens werken (boa’s met toezichthoudende taak).

  Daarnaast kunnen datalekken of actualiteiten aanleiding geven om een onderzoek op te starten. Met name AI zal in 2025 nauwlettend gevolgd worden. Bijvoorbeeld op de onderdelen beleid, training/voorlichting medewerkers en do’s en don’ts. Als altijd dient conform de AVG de FG tijdig en naar behoren betrokken te worden.

3. Organisatorische inbedding

Acties: blijvend verzorgen van presentaties aan teams om bewustzijn van omgang met persoonsgegevens op de agenda te houden. Het doel hierbij is om laagdrempelig vragen om advies in ontvangst te kunnen nemen. Waarop maatwerk qua advies gegeven kan worden. De filosofie van de FG en PO is en blijft dat er pragmatisch en oplossingsgericht geadviseerd wordt. Daarbij wordt de inhoudelijke AVG-kennis gekoppeld aan de organisatiekennis.

4. Rechten van betrokkenen

Actie: conform procedure zullen betrokkenen antwoord krijgen.

5. Samenwerking

Actie: het register met verwerkersovereenkomsten onderhouden in een toegankelijk portaal, zo nodig met verwijzing naar het bovenliggende contract.

6. Beveiliging

Informatiebeveiliging zorgt ervoor dat persoonsgegevens goed beveiligd zijn. In paragraaf 6 op pagina 7 van deze rapportage staat toegelicht volgens welke systematiek dat gebeurt. De jaarlijkse toetsing levert actiepunten op.
Acties: er wordt verwezen naar de actiepunten zoals die in de ENSIA-verantwoordingsrapportages benoemd zijn door de CISO. Deze ENSIA-verantwoordingsrapportages worden door de CISO aan College en Raad aangeboden.

7. Verantwoording

Actie: aan de bestuursorganen zal de stand van zaken gerapporteerd worden. Daarnaast zal de FG vanuit zijn toezichthoudende rol weer een jaarrapportage schrijven.

BIJLAGE 1 OVERZICHT UITGEVOERDE DPIA'S*en privacyscans in 2024

- iSamenleving
- Voertuigvolgsysteem
- Jonge Aanwas
- Woningverbetering Lelystad-Oost
- Klokkenluidersregeling / gedragscode ambtenaren
- DataMask (anonimiseringssoftware)
- Osint (Openbare bronnenonderzoek)
- Ondermijning
- Bodycams

De DPIA's zijn door de Privacy Officer uitgevoerd tezamen met een medewerker die inhoudelijk betrokken is bij het onderwerp. De DPIA wordt ter validatie aan de FG voorgelegd. Een DPIA wordt alleen uitgevoerd wanneer de aard van verwerking verandert en/of de verwerking van gegevens een hoog privacy risico met zich mee brengt.
Een privacyscan maakt inzichtelijk of en hoe er met persoonsgegevens gewerkt gaat worden in de beoogde applicatie.
Sommige DPIA's zijn in 2024 opgestart maar nog niet afgerond.

*DPIA staat voor Data Protection Impact Assessment

BIJLAGE 2 OVERZICHT RECHTEN VAN BETROKKENEN

In 2024 waren er 6 verzoeken om inzage van inwoners in alle persoonsgegevens die bij de gemeente worden verwerkt.

Alle verzoeken tot inzage in persoonsgegevens zijn naar tevredenheid afgehandeld. Geen van de beantwoordingen op verzoeken heeft tot aanvullende vragen of bezwaar geleid.

BIJLAGE 3 OVERZICHT DATALEKKEN

In 2024 zijn er 18 datalekken gemeld aan de FG. Die zijn conform procedure afgehandeld. In de gevallen waarin dat nodig was (mogelijk ernstige nadelige gevolgen voor de betrokkene) is het gemeld aan de betrokkenen en/of de Autoriteit Persoonsgegevens. Bij elk datalek wordt nagegaan of de onderliggende werkwijze aanpassing behoeft waardoor herhaling voorkomen kan worden. En wordt het intern besproken in het betreffende team om er lering uit te trekken. Datalekken worden standaard intern door de FG gemeld aan de gemeentesecretaris en betreffende wethouder(s).
Het betrof de volgende datalekken:

- energietoeslag aanvraag intern aan hele team gemaild
- BOA heeft delen gegevens in app gedeeld waarin ook onbevoegde in zat
- verkeerde clientgegevens in brief
- Geboorteakte aan verkeerde persoon gestuurd
- autorisaties Stipter Woonzorg stonden te ruim
- Data Solutions documenten verkeerd verstuurd
- 2 brieven onterecht geopend
- integriteitsmelding 2020 en 2023 was ten onrechte niet als datalek aangemerkt
- Data Solutions: brief abusievelijk geopend en ingescand (3x)
- Brief aan verkeerde persoon gestuurd per post
- Huwelijksakte naar oud adres opgestuurd
- uitnodiging naar verkeerde adres gestuurd
- Power BI (intern) stonden aantal autorisaties te ruim
- JCC Software: 7 mailadressen van (ex)-collega’s zijn buitgemaakt bij een cyberaanval
- Bewindvoerder ontving per ongeluk gegevens van aantal andere cliënten
- Verwerker ontving mail met teveel persoonsgegevens