JAARVERSLAG PRIVACY 2020 GEMEENTE APELDOORN

Juni 2021

Auteur: Ronald Schotanus (Concern Privacy Officer)

Algemene indruk 2020

De afgelopen jaren is in de gemeente Apeldoorn de basis gelegd om op een adequate wijze om te kunnen gaan met privacy en gegevensbescherming. De daaropvolgende fase is om privacy en gegevensbescherming daadwerkelijk onderdeel te laten worden van de dienstverlening, werkprocessen en de planning- en controlcyclus. Hoewel er zeker stappen worden gezet, kan nog niet gezegd worden dat de 'huishouding' op het gebied van privacy volledig op orde is. De risico's op het gebied van privacy zijn niet altijd voldoende in beeld en rond privacy is er veelal nog niet een continue verbeteringsproces ontstaan.

De gemeente bevindt zich nog niet op het volwassenheidsniveau waar de AVG van uitgaat. Bij dat niveau hoort ook de structurele uitvoering van data protection impact assessments (DPIA's) door de verwerkingsverantwoordelijke. Binnen de gemeente is de inzet van dit instrument om de risico's te beoordelen nog geen 'gemeengoed'. Er wordt daarmee nog niet voldoende gezorgd voor aantoonbare naleving van wet- en regelgeving. In plaats van te anticiperen en het willen voorkomen van bijvoorbeeld onrechtmatige verwerkingen of een datalek, wordt nog te veel gedacht dat er niks kan gebeuren of wordt te veel gehoopt op een goede uitkomst (een 'voorbijgaande storm').
Artikel 5 lid 2 AVG kent de verplichting om aan te tonen dat de uitgangspunten voor de verwerking van persoonsgegevens worden nageleefd.

Binnen de gemeente Apeldoorn bokst privacy ook nog geregeld op tegen de onterechte beeldvorming dat er niks meer mag. Vanuit de AVG is voor het verwerken en uitwisselen van gegevens veel mogelijk, als de inrichting en het borgen van de spelregels maar goed geregeld wordt. De domeinspecifieke wetgeving bevat vaak de echte regels voor de wijze waarop er met gegevens kan of moet worden gewerkt.

Een goede omgang met privacy biedt kansen processen te optimaliseren, data op te schonen en het risico op incidenten te verminderen. Om dat niveau te bereiken is onder meer nodig:
- het tijdig betrekken van privacy bij nieuwe ontwikkelingen;
- voldoende capaciteit (binnen afdelingen) voor privacy;
- meer duidelijkheid over de verantwoordelijkheden op het niveau van lijnmanagement en de onafhankelijke rol van de Concern Privacy Officer (CPO) en Functionaris Gegevensbescherming (FG).

Risico's op het gebied van privacy kunnen aanwezig zijn bij onder meer: de manier van werken in het stadhuis, toepassingen in het kader van Smart City, gegevensuitwisseling binnen het zorg- en veiligheidsdomein, de inrichting van Samen055, autorisatiebeheer (waaronder logging en controle), data analyses, het niet uitvoeren van verplichte DPIA's, handhaving van bewaartermijnen, de werking van samenwerkingsverbanden en de inzet van cameratoezicht.

Dit jaarverslag bevat een kritisch geluid van wat de CPO en FG binnen de organisatie zien. De insteek daarbij is niet om in problemen te denken, maar duidelijk is wel dat er voor de naleving van privacyregels nog de nodige stappen moeten worden gezet.

Leeswijzer

STATUS PRIVACY

- Bestuurlijke uitgangspunten
- Stand van zaken op basis van 7 hoofdthema’s
- Overzicht DPIA’s, rechten van betrokkenen en datalekken

Status privacy

BESTUURLIJKE UITGANGSPUNTEN
Bestuurlijke principes en beleid, werking en naleving

Het bestuur van deze gemeente:

- Zorgt voor het borgen van de Algemene Verordening Gegevensbescherming (AVG) en andere wet- en regelgeving op het gebied van privacy binnen de gemeentelijke organisatie.
- Zorgt ervoor dat de zorgvuldige en rechtmatige omgang met persoonsgegevens door de gemeentelijke organisatie wordt uitgevoerd;
- Controleert de juiste werking van privacy.

Het onderwerp 'privacy' is opgesplitst in 7 thema's, welke gezamenlijk alle aspecten van gegevensbescherming dekken. Er is geen volgorde: de criteria dienen in onderlinge samenhang te worden gelezen.
Bij het in beeld brengen van de stand van zaken worden de volgende kleuren gebruikt:

 managementaandacht nodig

 gedeeltelijk op orde

 in control

1. BELEID Actueel beleid met de vastgestelde kaders	
2. PROCESSEN Privacy is een regulier onderdeel van de dienstverlening en werkprocessen	
3. ORGANISATORISCHE INBEDDING Toewijzing van taken, verantwoordelijkheden en bevoegdheden	
4. RECHTEN VAN BETROKKENEN Transparantie en het faciliteren van de rechten die betrokkenen hebben	
5. SAMENWERKING Juiste afspraken met samenwerkende partners	
6. BEVEILIGING Er worden passende technische en organisatorische maatregelen getroffen	
7. VERANTWOORDING Aantonen dat de organisatie voldoet aan de privacyregels	

1. BELEID

Het privacybeleid is een kader waarin wordt aangegeven aan welke principes de gemeente zich ten aanzien van privacy houdt. Het laat zien hoe de organisatie omgaat met persoonsgegevens en welke maatregelen worden getroffen om te voldoen aan wet- en regelgeving.

Status: gedeeltelijk

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

Bestuur, directie en management laten zien dat privacy belangrijk is en zijn actief betrokken	○ ● ○
Er is een algemeen privacybeleid met de vastgestelde kaders	○ ○ ●
Het privacybeleid is leidend bij ontwerp en ontwikkelingen van (nieuwe) verwerkingen	○ ● ○

Bevindingen

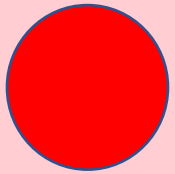
De verantwoordelijk portefeuillehouder is actief betrokken op het gebied van privacy. Vanuit directie en het management wordt vaak gesteld dat privacy en een zorgvuldige omgang met gegevens belangrijk wordt gevonden, echter wordt privacy niet altijd tijdig en naar behoren betrokken bij (nieuwe) ontwikkelingen en worden er nog geregeld risico's op 'niet voldoen' geaccepteerd.

Er is een vastgesteld privacybeleid voor de gemeente Apeldoorn, dit beleid is ook gepubliceerd via de gemeentelijke website. In de volgende versie van het privacybeleid is het goed meer aandacht te geven aan rollen en verantwoordelijkheden.

Nieuwe ontwikkelingen, verwerkingen of wijzigingen van verwerkingen worden niet altijd voorafgaand getoetst aan de uitgangspunten van het privacybeleid en geldende wet- en regelgeving. Wanneer privacy in het ontwerp te laat wordt betrokken, leidt dit geregeld tot een onterechte bevinding dat er van de AVG niks meer mag.

2. PROCESSEN

Status:
aandacht nodig



De verwerkingen van persoonsgegevens door de gemeente dienen te voldoen aan de uitgangspunten van de AVG. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten getoetst en ingericht moeten worden volgens de beginselen: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid.
Daarnaast kan de verwerkingsverantwoordelijke verplicht zijn om een zogenoemde 'data protection impact assessment' (DPIA) uit te voeren.

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

Er zijn passende instructies voor medewerkers over de omgang met persoonsgegevens in (kritische) werkprocessen	○ ● ○
Het verwerkingsregister is actueel en het beheer is intern belegd	○ ● ○
Voor verwerkingen (met hoge privacyrisico's) worden DPIA's en de benodigde mitigerende maatregelen uitgevoerd	● ○ ○

Bevindingen

Privacy en gegevensverwerking is een organisatievraagstuk. Als processen goed ingeregeld zijn, vallen heel veel vragen over wat wel / niet mag voor gegevensverwerking- of uitwisseling ook weg. Niet in alle werkprocessen- of instructies zijn afspraken over de omgang of een eenduidige manier van werken met persoonsgegevens binnen het betreffende team vastgelegd. Het verwerkingsregister kan meer helpen om het proces ingericht te krijgen.

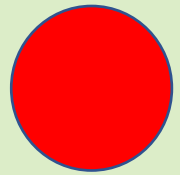
Het verwerkingsregister wordt decentraal niet door alle afdelingen actief beheerd en jaarlijks vastgesteld, het centrale verwerkingsregister is nog niet als publieke versie gepubliceerd.

Voor de uitvoering van data protection impact assessments (DPIA's), een instrument om risico's vooraf in beeld te krijgen, is een format (quickscan, procedure, vragenlijst, rapportage) beschikbaar, maar veelal is niet bekend dat de opdrachtgever of proceseigenaar zelf verantwoordelijk is voor de uitvoering daarvan. Het is wenselijk dat er een inventarisatie plaatsvindt waar DPIA's nodig zijn en dat er en planning voor de uitvoering komt.
Aan het einde van dit jaarverslag is een overzicht opgenomen van de uitgevoerde DPIA's voor het jaar 2020.

Áan het niet uitvoeren van DPIA's wordt risicogericht een groter gewicht toegekend, waardoor het resultaat van dit thema op 'aandacht nodig' staat.

3. ORGANISATORISCHE INBEDDING

Status:
aandacht nodig



Het is van belang dat iedereen binnen de organisatie op de hoogte is van het belang van een goede omgang met persoons-gegevens. Organisatorische inbedding betekent het toewijzen van taken, verantwoordelijkheden en bevoegdheden en het creëren van bewustzijn.

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

Er is ruime (juridische) kennis over privacy, gegevensbescherming en relevante wet- en regelgeving	● ○ ○
Er zijn voldoende middelen beschikbaar om privacy bewustzijn te bevorderen in kennis, houding en gedrag van de medewerkers	○ ● ○

Bevindingen

Het aantal medewerkers dat zich met privacy bezighoudt is beperkt. Bovendien zijn er weinig afdelingen die zelf hun eigen verantwoordelijkheid voor privacy vraagstukken op casusniveau pakken. Voor de grootte van een organisatie als de gemeente Apeldoorn is de capaciteit voor privacy niet voldoende. Hoe groot de benodigde capaciteit wel zou moeten zijn, is mede afhankelijk van het ambitieniveau van de organisatie op dit vlak.

In 2020 zijn er verschillende activiteiten uitgevoerd voor het vergroten van bewustwording, maar meer aandacht daarvoor is gewenst om de medewerkers structureel bewust te laten zijn van de privacy aspecten binnen hun werk. Zodra (eigen) gegevens van medewerkers geraakt worden, is het 'alle hens aan dek', maar risico's op nadelige gevolgen voor anderen (inwoners of andere betrokkenen) worden nog niet altijd gezien of naar waarde geschat.

Voor het bevorderen van bewustwording lopen reeds (verbeter)acties, waardoor het andere criteria een groter gewicht heeft gekregen bij de beoordeling van het resultaat van dit thema.

4. RECHTEN VAN BETROKKENEN

Status: gedeeltelijk

Inwoners, medewerkers en andere betrokkenen moeten zowel actief als passief geïnformeerd worden over de omgang met hun persoonsgegevens. Daarnaast stelt de AVG betrokkenen in staat om middels een aantal rechten controle en invloed uit te oefenen over zijn of haar persoonsgegevens.

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

Er is een werkend proces om de rechten van betrokkenen te faciliteren	○ ● ○
Betrokkenen worden voorafgaand aan een verwerking actief, tijdig en adequaat geïnformeerd	○ ● ○

Bevindingen

De uitvoering van het proces voor het voldoen aan de rechten van betrokkenen (bijvoorbeeld een inzageverzoek) gaat steeds beter, in enkele gevallen is het nog lastig om binnen de wettelijke termijnen de benodigde gegevens en/of documenten boven tafel te krijgen.

Transparantie is een van de belangrijkste uitgangspunten van de AVG. Op de gemeentelijke website is een algemene privacyverklaring opgenomen. Voorafgaand aan een specifieke verwerking worden betrokkenen nog niet altijd geïnformeerd over de soort gegevens die worden verwerkt, de bron van de gegevens, het doel van de verwerking, de grondslag van de verwerking, aan wie de gegevens worden verstrekt. Er kan nog meer worden uitgegaan van het uitgangspunt 'met de burger in plaats van over de burger'.

Aan het einde van dit jaarverslag is een overzicht opgenomen van het aantal verzoeken van burgers voor het jaar 2020.

5. SAMENWERKING

Status: gedeeltelijk

De gemeente werkt op meerdere beleidsterreinen samen met (mede-)overheden, ketenpartners en private organisaties. Juiste afspraken over de omgang met persoonsgegevens zijn nodig met samenwerkende partijen.

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

De organisatie heeft inzichtelijk met welke partijen er sprake is van het verwerken van persoonsgegevens	○ ● ○
Bij het inschakelen van externe partijen wordt voorafgaand getoetst of er sprake is van het verwerken van persoonsgegevens en wanneer dit het geval is, worden voorafgaand aan de inschakeling afspraken gemaakt over de verwerking	○ ● ○

Bevindingen

Een volledig overzicht van samenwerkingen waarbij er sprake is van het verwerken van persoonsgegevens met externe partijen ontbreekt, ook voor situaties waarbij de gemeente Apeldoorn mogelijk een taak of verantwoordelijkheid heeft voor gegevensbescherming. Bij meerdere bestaande samenwerkingen moeten gemaakte afspraken geactualiseerd en aangevuld worden met nadere afspraken over privacy, gegevensuitwisseling en de rol die de betrokken partijen innemen.

De standaard verwerkersovereenkomst is beschikbaar en voldoet aan de landelijk gemaakte VNG-afspraken. Het afsluiten van verwerkersovereenkomsten met nieuwe partijen gaat over het algemeen goed. Afspraken met andere zelfstandig verantwoordelijken of afspraken in situaties van gezamenlijke verwerkingsverantwoordelijkheid vraagt zeker nog de nodige aandacht.

6. BEVEILIGING

Passende technische en organisatorische maatregelen zijn essentieel om persoonsgegevens te beschermen. De basis voor passende beveiliging ligt in de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast geldt er onder de AVG een meldplicht datalekken. Dit houdt in dat incidenten waar persoonsgegevens bij betrokken zijn onder omstandigheden gemeld dienen te worden aan de Autoriteit Persoonsgegevens en/of betrokkenen.

Status: gedeeltelijk

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

De gemeente heeft een werkend proces datalekken en inzicht in alle inbreuken op persoonsgegevens

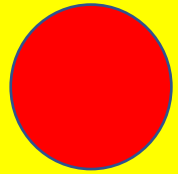
Bevindingen

Via bewustwordingsactiviteiten is regelmatig aandacht gevraagd voor het melden van datalekken. Alle gemelde datalekken worden intern geregistreerd en, wanneer nodig, gemeld aan de Autoriteit Persoonsgegevens en/of betrokkenen. In vergelijking met landelijke cijfers is het totaal aantal datalekken in Apeldoorn relatief laag, ook is voor een aantal oorzaken (bv. mail aan verkeerde ontvanger) bij meerdere processen nog een betere opvolging voor verbetering mogelijk.

Aan het einde van dit jaarverslag is een overzicht opgenomen van het aantal datalekken in het jaar 2020.

7. VERANTWOORDING

Status: gedeeltelijk



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 gemeente een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy. Dit betekent dat de gemeente aan moet kunnen tonen dat de verwerkingen van persoonsgegevens voldoen aan de beginselen van de AVG en andere relevante wet- en regelgeving.

Onderdelen:

managementaandacht nodig | gedeeltelijk op orde | in control

De gemeente heeft inzichtelijk welke acties en maatregelen genomen moeten worden om het niveau van gegevensbescherming en de zorgvuldige omgang met persoonsgegevens naar een hoger niveau te brengen.	
Verantwoording is structureel ingericht, zodat naleving is geborgd	

Bevindingen

In 2020 is met alle afdelingen een nulmeting (toetsplan) voor de borging van privacy binnen de organisatie uitgevoerd. De resultaten daarvan zullen in 2021 besproken en meegenomen worden in de periodieke bedrijfsvoeringsrapportages.

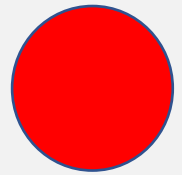
Hoewel op verschillende niveaus over de voortgang van verbeteracties en relevante ontwikkelingen op het gebied van privacy wordt gerapporteerd, is er nog niet in alle gevallen sprake van een continue verbetercyclus. Ook doordat er weinig DPIA's zijn uitgevoerd, wordt nog niet voldoende gezorgd voor aantoonbare naleving van wet- en regelgeving. De verantwoording is vooral een verantwoordelijkheid van de primaire afdelingen.

Een aandachtspunt met betrekking tot de verantwoording is dat, wanneer de verwerkingsverantwoordelijke in voorkomende gevallen afwijkt van het advies van de CPO of FG, de motivering daarvan altijd vastgelegd dient te worden.

Voor het eerste criterium zijn (verbeter)acties in gang gezet, aan het inrichten van de verantwoording (deels via DPIA's) is het meeste gewicht toegekend bij de beoordeling van het resultaat van dit thema.

Overzicht DPIA's

Status werking: aandacht nodig



De AVG beschrijft in artikel 35 dat organisaties een data protection impact assessment (DPIA) moeten uitvoeren wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt (of kan inhouden) voor de rechten en vrijheden van personen. Een DPIA is een instrument om vooraf privacyrisico's in kaart te brengen, om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Op het niet uitvoeren van een verplichte DPIA staat een boete (beginnend bij 310.000 euro).

Het advies van de Autoriteit Persoonsgegevens is om periodiek een DPIA uit te voeren op bestaande gegevensverwerkingen, in ieder geval elke 3 jaar. Deze termijn is begonnen op 25 mei 2018 (datum inwerkingtreding AVG).

Hieronder staat een overzicht van de DPIA's die in 2020 zijn uitgevoerd of waar een begin mee is gemaakt:

Onderwerp DPIA	**Status**
Stadspas	In 2020 gestart, inmiddels afgerond
Wvggz	Afgerond
Djuma	In behandeling
Bodycams	Afgerond

De nieuwe applicatie voor burgerzaken is in 2020 geïmplementeerd, hier is geen DPIA voor uitgevoerd. Ook voor de camera's in het stadhuis en de parkeergarages is geen DPIA uitgevoerd.
Voor bestaande verwerkingen is nog geen DPIA uitgevoerd dan wel mee gestart.

Overzicht rechten van betrokkenen

Status werking: gedeeltelijk

Onder de voorlopende Wet bescherming persoonsgegevens hadden burgers al het recht geïnformeerd te worden over het gebruik van hun persoonsgegevens. Daarnaast kunnen zij inzage en rectificatie van hun gegevens vragen of bezwaar maken tegen het gebruik ervan. Onder de AVG zijn hier nog twee belangrijke rechten bijgekomen, namelijk het recht op overdraagbaarheid en het recht op vergetelheid.

Uitgangspunt is dat de diverse rechten de betrokkene in staat kunnen stellen om na te gaan welke gegevens met welke herkomst worden verwerkt en deze zo nodig te corrigeren of te verwijderen.

In 2020 zijn in totaal 5 verzoeken tot uitoefening van een recht ingediend bij de gemeente Apeldoorn. Hieronder wordt een overzicht getoond met het aantal verzoeken van betrokkenen in 2020 om uitoefening van een recht:

Recht	Aantal	Opmerking
Inzage, algemeen verzoek	2	Beide inzageverzoeken bleken inwoners van de gemeente Epe en Brummen te betreffen. Voor deze gemeenten voert Apeldoorn meerdere taken in het sociaal domein uit. Deze verzoeken zijn ter afhandeling doorgestuurd naar de betreffende gemeenten.
Vergetelheid	3	1 verzoek is niet gehonoreerd doordat betrokkene niet aan identificatieplicht heeft voldaan. Bij de andere 2 verzoeken is de beslissing genomen de gegevens te verwijderen nadat de vastgestelde bewaartermijn verlopen is.

Geen van deze verzoeken hebben geleid tot vervolgacties, bijvoorbeeld om gegevens te corrigeren.

Inzageverzoeken op basis van de AVG worden nog niet altijd direct als dusdanig herkend. Ook levert de afhandelingstermijn van 4 weken nog wel eens problemen op voor het bij elkaar krijgen van de juiste documenten en/of gegevens.

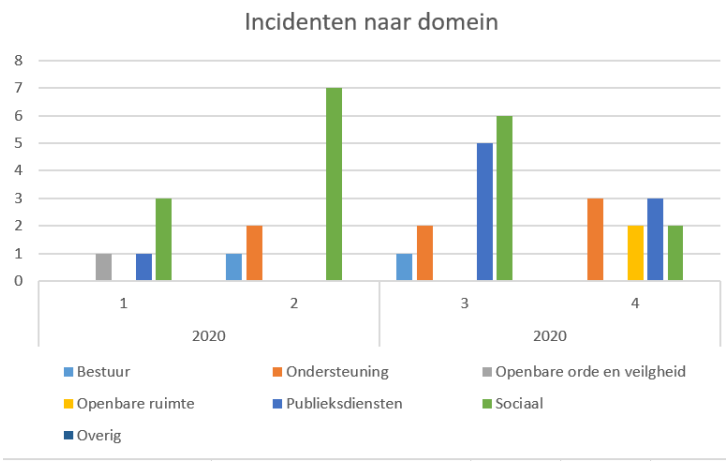
Naast bovengenoemde verzoeken zijn er in 2020 ook meerdere vragen en klachten van inwoners afgehandeld, zowel telefonisch als per mail.

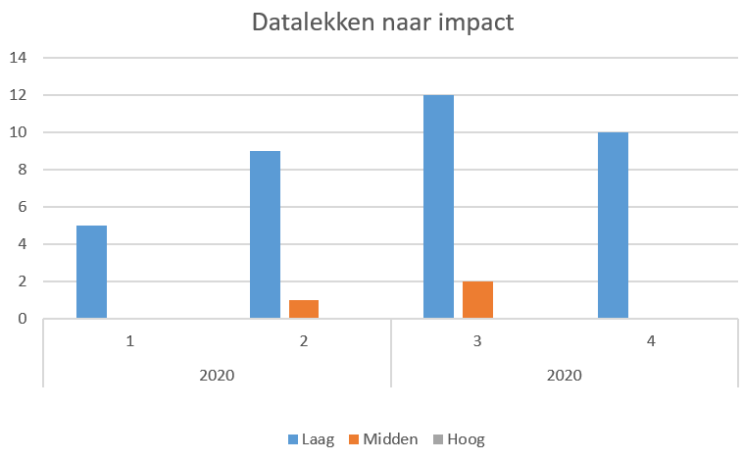
Overzicht datalekken

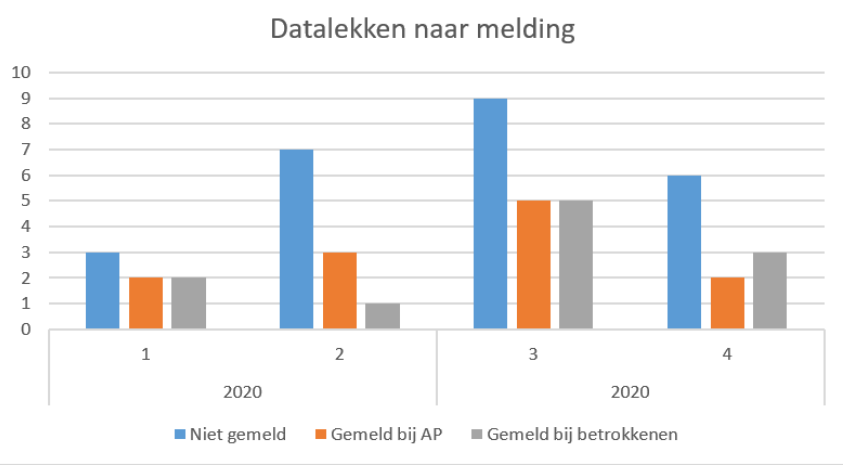
De meldplicht datalekken geldt sinds 2016 en vloeit ook voort uit AVG. De gemeente moet alle datalekken documenteren, inclusief de feiten over het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Er is sprake van een datalek als er naar een persoon herleidbare informatie bij iemand terecht komt waarbij dat niet de bedoeling is.

Status werking: gedeeltelijk

In 2020 zijn er binnen de gemeente Apeldoorn in totaal 40 datalekken geregistreerd (1). Hieronder zijn deze gevisualiseerd in een overzicht wat betreft het betrokken domein, de impact en het feit of het datalek al dan niet gemeld is bij de Autoriteit Persoonsgegevens. Bij de datalekken met hogere impact en/of melding bij de AP ging het om een niet openbaar stuk op het Raadsinformatiesysteem en om onrechtmatige verstrekkingen of onbevoegde raadplegingen van vertrouwelijke informatie of gevoelige gegevens. In 2020 is 1 datalek in de regionale media gekomen: https://www.destentor.nl/apeldoorn/woede-in-ugchelen-over-datalek-gemeente-apeldoorn-mailt-namen-bezwaarmakers-naar-projectontwikkelaar~a771527f/







Nog niet alle voorkomende datalekken worden intern gemeld.

1 Ter vergelijking: in 2018 zijn er in totaal 21 datalekken geregistreerd, in 2019 zijn dat er in totaal 37 geweest.

Voorbeelden van datalekken in 2020 binnen Apeldoorn

- Mail met gegevens over beschermingsbewind verstuurd aan een verkeerde ontvanger;
- Meer persoonsgegevens (van bezwaarmakers tegen ontwerp bestemmingsplan) dan noodzakelijk gedeeld met een projectontwikkelaar;
- Toegang in het systeem tot personeelsdossier van andere medewerker;
- Persoonslijst (BRP) per post verzonden aan verkeerde ontvanger;
- Bij online opvragen geboorteakte werden de gegevens van een ander kind getoond;
- Telefonisch onterecht gevoelige informatie van een burger verstrekt aan een instantie.