Geschillenkamer

Beslissing ten gronde 19/2020 van 29 april 2020

Dossiernr. : DOS-2018-05421

Betreft: Klacht tegen een gemeente over de rechtmatigheid van de raadpleging van een burgerfoto in het Rijksregister door een gemeentemedewerker

De Geschillenkamer van de Gegevensbeschermingsautoriteit, bestaande uit de heer Hielke Hijmans, voorzitter, en de heren Y. Poullet en C. Boeraeve, leden. De zaak is in deze samenstelling opgenomen.

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming, hierna "AVG");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit (hierna GBA-wet*);

Gelet op de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*. ;

Gelet op het reglement van interne orde, zoals goedgekeurd door de Kamer van Volksvertegenwoordigers op 20 december 2018 en gepubliceerd in het Belgisch Staatsblad op 15 januari 2019;

Gelet op de stukken van het dossier;

Heeft de volgende beslissing genomen inzake:

- De klager
- De verwerkingsverantwoordelijke (hierna de verweerder):

I. Historiek van de procedure

Gelet op de klacht van 2 september 2018 die de klager heeft ingediend bij de Gegevensbeschermingsautoriteit;

Gelet op de beslissing van 26 oktober 2018 van de Eerstelijnsdienst van de Gegevensbeschermingsautoriteit om de klacht ontvankelijk te verklaren en deze op dezelfde datum door te sturen naar de Geschillenkamer;

Gelet op de beslissing die de Geschillenkamer heeft genomen tijdens haar zitting van 14 november 2018 om, in toepassing van de artikelen 63,2° en 94, 1° van WOG aan de Inspectiedienst een onderzoek te vragen; Gelet op de verwijzing van het dossier naar de Inspecteur-generaal op diezelfde datum;

Gelet op het verslag en het proces-verbaal van het onderzoek van de Inspecteur-generaal, die op 17 mei 2019 aan de Geschillenkamer zijn toegezonden;

Gelet op de beslissing die de Geschillenkamer tijdens haar zitting van 28 oktober 2019 heeft genomen om het dossier ten gronde te behandelen op grond van de artikelen 95 § 1, 1° en 98 van de WOG;

Gelet op de mededeling, op 29 mei 2019 van het verslag en het proces-verbaal van het onderzoek van de Inspecteur-generaal aan de partijen en het verzoek van de Geschillenkamer aan de partijen om hun argumenten te formuleren volgens een vastgesteld tijdschema; Gelet op de beslissing van 19 juli 2019 van de Geschillenkamer om de uiterste datum van de neerlegging van de conclusies voor de verweerder te verplaatsen van 19 juli 2019 naar 19 augustus 2019;

Gelet op de conclusies op 19 augustus 2019, neergelegd door de raadsmannen van de verweerder en de bijhorende e-mail waarin de raadsmannen van de verweerder verklaren dat hun cliënt gehoord wenst te worden in toepassing van artikel 51 van het Reglement van interne orde van de Gegevensbeschermingsautoriteit;

Gelet op de hoorzitting tijdens de zitting van 18 november 2019 waar de verweerder, vertegenwoordigd door zijn raadsman is verschenen. Aan het einde van deze zitting heeft de

Geschillenkamer besloten de zaak voort te zetten en heeft zij de verweerder verzocht haar alle aanvullende documenten te doen toekomen waaruit blijkt dat de laatste maatregelen werden ingevoerd sinds de neerlegging van zijn conclusies in augustus 2019 ;

Gelet op het proces-verbaal van 18 november 2019;

Gelet op de bijkomende stukken, neergelegd door de verweerder op 22 en 26 november 2019;

Gelet op de brief en het antwoord van de klager van 11 december 2019;

Gelet op de laatste neergelegde stukken als repliek van de verweerder op 14 januari 2020.

II. Feiten en voorwerp van de klacht

Volgens zijn klacht stelt de klager dat hij twijfelt aan de rechtmatigheid van de raadpleging van zijn foto in het Rijksregister op 11 mei 2018 door een medewerker van de verweerder. Op 27 juni 2019 stuurt hij een e-mail naar de helpdesk Belpic (FOD Binnenlandse Zaken - Algemene Directie Instellingen en Bevolking, in deze bewoordingen:

> *"Mevrouw, Mijnheer,*
> *Bij het raadplegen van mijn dossier via IBZ, stel ik vast dat een raadpleging in " Code transactie 08 - Raadpleging foto" plaatsvond op 11/05/2018 om 14:39 uur.*
>
> *Wetende dat ik op dat moment op huwelijksreis was, vind ik het nogal vreemd dat iemand mijn foto raadpleegt.*
>
> *(...) dus ik weet uit ervaring dat men geen transactiecode 08 raadpleegt zonder geldige reden. Het gaat zeker om een collega, dus ik zou daar graag meer willen weten als dat mogelijk is. (…) ».*

Op 28 juni antwoordt de Helpdesk Belpic per e-mail het volgende:

> *"De personeelsleden van de instanties die gemachtigd zijn toegang te hebben tot de gegevens in het Rijksregister, zijn gebonden aan het beroepsgeheim. Het onrechtmatig raadplegen van dossiers (bijvoorbeeld voor privédoeleinden) brengt hun persoonlijke verantwoordelijkheid op disciplinair, burgerlijk en strafrechtelijk vlak in het geding.*
>
> *Als u vermoedt dat een instantie uw gegevens onjuist of onreglementair gebruikt, kunt u rechtstreeks contact opnemen met de organisatie. De instanties moeten namelijk zorgen voor de traceerbaarheid en de archivering van de raadplegingen die bij hen worden uitgevoerd en*

zullen u normaal gesproken informatie kunnen verstrekken over de aard van deze raadplegingen.

Als het antwoord niet bevredigend is of als u ernstige redenen hebt om aan te nemen dat het een onterechte raadpleging betreft, kunt u een klacht indienen bij de Commissie voor de bescherming van de persoonlijke levenssfeer (https://www.privacycommission.be/fr) of bij een rechtbank.

De diensten van het Rijksregister beschikken over het algemeen niet over informatie over de raadplegingen die door deze instanties worden uitgevoerd en zijn bovendien niet bevoegd om de klachten te behandelen".

Eveneens per e-mail van 28 juni 2019 richtte de klager zich tot een vroegere collega, om te weten naar wie hij zijn verzoek bij de verweerder diende te richten. Zonder antwoord, herhaalt de klager zijn verzoek per e-mail op 14 augustus 2019. Bij e-mail van 29 augustus 2019 werd de verweerder ervan in kennis gesteld dat een onderzoek was aangevraagd en dat de klager op een later tijdstip op de hoogte zou worden gesteld van het resultaat van het onderzoek.

De klager informeerde per e-mail van 27 september 2019 naar het resultaat van zijn verzoek. Op 27 september 2019 ontving hij het volgende antwoord:

« Dag,
Een onderzoek werd opgestart maar leverde geen totale zekerheid op noch wat betreft de persoon die uw dossier consulteerde (alleen de foto), noch wat betreft de eventuele motivatie voor de raadpleging.
Er werden geen bekentenissen afgelegd. De feiten werden evenwel geacteerd".

Vrije vertaling naar het Frans:
« Bonjour,
Une enquête a été ouverte mais n'a pas apporté de certitude absolue ni concernant la personne qui a consulté votre dossier (uniquement la photo) ni la motivation éventuelle de la consultation.
Aucun n'aveu n'a été fait. Toutefois les faits ont été actés ».

Op 2 oktober 2019 diende de klager een klacht in bij de Gegevensbeschermingsautoriteit.

III. Het verslag en het proces-verbaal van het onderzoek van de Inspecteur-generaal

Met zijn verslag en proces-verbaal van het onderzoek van 17 mei 2019, stelt de Inspecteur-generaal het volgende vast:

> *Vaststelling 1 : de verweerder heeft de betwiste raadpleging overeenkomstig artikel 17 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van natuurlijke personen niet kunnen rechtvaardigen. In dit verband geeft het consultatieregister niet aan voor welk doel de gegevens in het Rijksregister zijn geraadpleegd.*

In het verslag wordt ook verwezen naar de verwijzing van de verweerder naar *Aanbeveling 07/2017 van 30 augustus 2017 van de Commissie voor de bescherming van de persoonlijke levenssfeer aan de steden en gemeenten over de registratie van de reden voor de raadpleging van het Rijksregister door hun personeelsleden*. [1] Per brief van 19 februari 2019 gericht aan de functionaris voor gegevensbescherming (DPO) van de verweerder, verzocht de Inspecteur-generaal immers om hem *"de redenen toe te lichten waarom geen concreet antwoord werd gegeven op de vraag van de burger (lees klager) (zie Aanbeveling 07/2017 van 30 augustus 2017 van de Commissie voor de bescherming van de persoonlijke levenssfeer aan de steden en gemeenten over de registratie van de reden voor de raadpleging van het Rijksregister door hun personeelsleden (CO-AR-2017-013)"*.

De verweerder verklaart in zijn antwoord van 29 april 2019 dat de controle die op basis van het verzoek van de klager is uitgevoerd, op 20 en 21 augustus 2019 is uitgevoerd door het SAPHIR-logboek te raadplegen dat wordt gebruikt voor de toegang tot het Rijksregister. Vervolgens werd een verzoek om uitleg gericht aan de ambtenaar onder wiens naam deze raadpleging werd geregistreerd, te weten de heer X, een werknemer van verweerder.

De verweerder stelt verder dat de reden waarom de identiteit van de ambtenaar die de foto van klager heeft geraadpleegd niet is bekendgemaakt, verband houdt met het gebrek aan absolute zekerheid dat deze ambtenaar in feite de persoon is die de foto heeft geraadpleegd. Dit gebrek aan absolute zekerheid is "te wijten aan het feit dat hij zich tijdens het verhoor niet kon herinneren dat hij deze raadpleging heeft uitgevoerd en hij preciseerde dat hij nooit foto's van burgers raadpleegt vanuit het Rijksregister, maar enkel in de Belpic-applicatie om een vergelijking te kunnen maken bij het bestellen van identiteitskaarten. De reden van de geregistreerde raadpleging kon niet worden vastgesteld" (Uittreksel van de brief van de verweerder van 29 april 2019 gericht aan de Inspecteur-generaal van de GBA).

[1] Deze aanbeveling is gepubliceerd op de website van de Gegevensbeschermingsautorieit en ook op de website van de Commissie voor de bescherming van de persoonlijkelevenssfeer na de aanname ervan in augustus 2017: https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_RR_01_2015.pdf

Ten slotte voegt de verweerder toe, nog steeds in het kader van de inspectie, dat er verschillende elementen aantonen waaruit blijkt dat hij sedert 2018 het bewustzijn en de verantwoordingsplicht van de ambtenaren bevordert die in de uitoefening van hun functie toegang krijgen tot het Rijksregister. In dit verband wijst hij erop dat de systematische registratie van het doel waarvoor de gegevens in het Rijksregister worden geraadpleegd, nog niet verplicht is gesteld. Het mechanisme ter bestrijding van ongegronde toegang is in wezen preventief van aard, zonder een actieve opsporing in het logboek, tenzij op verzoek van een burger.

In het inspectieverslag wordt in dit verband opgemerkt dat verweerder zich verbindt tot het volgende :

> *"Er zal een aanbeveling worden gedaan om het invoeren van de reden van de raadpleging verplicht te stellen. (...). Daarom zal ook een aanbeveling worden gedaan om het systeem aan te vullen met een detectielaag, gebaseerd op het principe dat de reden die in het toegangslogboek is vastgelegd, moet worden gestaafd met een concreet element, zoals een dossier, een verzoek, enz. en dat een steekproefcontrole ervoor kan zorgen dat dit het geval is." (Uittreksel uit het inspecieverslag - antwoord van de verweerder van 5 april 2019 - advies van de DPO).*

IV. Hoorzitting van 18 november 2019

Tijdens de hoorzitting van 18 november 2019 heeft de verweerder, via zijn raadsman, de argumenten uiteengezet die hij in zijn betoog van 19 augustus 2019 had ontwikkeld. Met name de raadsmannen van de verweerder geven toe dat er inderdaad een probleem is ontstaan bij het raadplegen van de foto van de klager. De verweerder wijst ook op de ernst waarmee de klacht van klager is behandeld en de daaraan gekoppelde besliste maatregelen werden ingevoerd of binnenkort zullen worden ingevoerd om te voldoen aan artikel 17 van de Rijksregisterwet.

IN RECHTE

V. Wat betreft de bevoegdheid van de Gegevensbeschermingsautoriteit, in het bijzonder de Geschillenkamer

In toepassing van artikel 4, §1 van de WOG, is de Gegevensbeschermingsautoriteit (GBA) verantwoordelijk voor het toezicht op de naleving van de grondbeginselen van de bescherming van de persoonsgegevens als vervat in de AVG en van de wetten die bepalingen bevatten inzake de bescherming van persoonsgegevensverwerkingen, waaronder de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*.

In toepassing van artikel 33, §1 van de WOG, is de Geschillenkamer het administratief geschillenorgaan van de GBA. Zij ontvangt de klachten die de Eerstelijnsdienst (ELD) haar overeenkomstig artikel 62 §1 van de WOG toezendt, d.w.z. de ontvankelijk klachten. Overeenkomstig

artikel 60, 2de lid van de WOG, zijn de klachten ontvankelijk als zij overeenkomstig artikel 60, §2 van de WOG in een van de nationale talen zijn opgesteld, een uiteenzetting bevatten van de feiten en de informatie die nodig is om de verwerking van de persoonsgegevens waarop zij betrekking hebben te identificeren en die onder de bevoegdheid vallen van de GBA.

De raadpleging van de foto waarvan de klager aangifte deed, dateert van 11 mei 2018. Deze raadpleging vond dus plaats voor de AVG van toepassing werd. De Geschillenkamer is daarom niet bevoegd om er kennis van te nemen. De Geschillenkamer vindt de rechtstgrond van haar bevoegdheid immers in de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* (WOG) waarvan de inwerkingtreding werd vastgesteld, behoudens uitzonderingen, op 25 mei 2018 (artikel 110 van de WOG). Hoewel de Geschillenkamer bevoegd is voor gegevensverwerkingen die weliswaar vóór 25 mei 2018 zijn begonnen, maar vandaag nog steeds doorgaan, is zij niet bevoegd voor eenmalige verwerkingen die vóór 25 mei 2018 zouden hebben plaatsgevonden, aangezien er geen sprake is van terugwerkende kracht in de tijd voor de uitoefening van haar bevoegdheid.

In het onderhavige geval heeft de inspectie die na de indiening van deze klacht is uitgevoerd, zoals uiteengezet in punt III hierboven, inbreuken aan het licht gebracht na 25 mei 2018, die de Geschillenkamer dan ook gerechtigd is te onderzoeken (zie punt VI hieronder).

VI. Over de redenen voor de beslissing

Ten eerste, wat betreft de schending van de rechten van de verdediging waarop verweerder zich beroept.

In zijn conclusies van 19 augustus 2019 betreurt verweerder aanvankelijk dat de klager geen verweerschrift heeft ingediend (punt 10 van het betoog van verweerder). Zij voegt daaraan toe dat het, gezien de bewoordingen van de klacht van deze laatste, onmogelijk is om volledig te begrijpen waarvan hij wordt beschuldigd en, meer in het bijzonder, welke wettelijke bepalingen er zouden zijn geschonden.

Bijgevolg is de verweerder van mening dat zijn rechten van verdediging in de onderhavige zaak niet zijn geëerbiedigd.

Tijdens de hoorzitting van 18 november 2019 heeft de verweerder zijn spijt en bezwaren in dit verband herhaald.

De Geschillenkamer is overigens van mening dat van een klager niet kan worden verlangd dat hij op een duidelijke, nauwkeurige en volledige wijze de wettelijke bepalingen aanwijst ter ondersteuning waarvan hij zijn klacht indient. Deze kwalificatie van de feiten - die desgevallend een inbreuk op de geldende regelgeving inzake de bescherming van persoonsgegevens vormt - valt onder de verantwoordelijkheid van de Inspectiedienst en de Geschillenkamer. In dit verband vraagt de Inspecteur-generaal in zijn brief van 19 februari 2019 aan de verweerder waarom hij zich niet heeft

gehouden aan de Aanbeveling 07/2017, waarin duidelijk wordt gesteld dat de vermelding van de reden van de raadpleging een garantie, noodzakelijk en verplicht is voor legitieme toegang tot het Rijksregister.

Uit het antwoord van de verweerder van 25 april 2019 blijkt dat hij heeft begrepen waarvan hij wordt beschuldigd. In het op 29 mei 2019 aan de verweerder meegedeelde inspectieverslag wordt nogmaals naar deze aanbeveling verwezen. Ten slotte heeft de verweerder in punt 11 van zijn antwoord, niettegenstaande zijn inleidend verweer, vermeld: "*Ondanks het bovenstaande lijken er twee vragen te komen uit de klacht die werd ingediend op 2 oktober 2018:*

- *De identiteit van de auteur van de betwiste raadpleging in het Rijksregister;*
- *De redenen voor deze raadpleging, voor zover de klager twijfelt aan het verband tussen deze raadpleging en zijn ontslag, dat hij als onrechtmatig beschouwt* ».

De verweerder verdedigt zich vervolgens met betrekking tot die klachten in zijn conclusies.

Concluderend kan in het licht van het voorgaande niet worden gesteld dat de rechten van de verdedigng van de verweeder niet zijn gerespecteerd.

*

Over de noodzakelijke naleving van het verantwoordingsplichtbeginsel (artikel 5, § 2 en 24 van de AVG) en de veiligheidsverplichting (artikel 32 van de AVG en artikel 17 van de Wet tot regeling van een Rijksregister van de natuurlijke personen), gekoppeld aan het finaliteitsbeginsel (artikel 5, § 1, b), van de AVG) en het veiligheidsbeginsel (artikel 5, § 1, f), van de AVG)

Als verwerkingsverantwoordelijke is de verweerder verplicht de gegevensbeschermingsbeginselen in acht te nemen en moet hij kunnen aantonen dat deze beginselen worden nageleefd (verantwoordingsplichtbeginsel - artikel 5.2 van de AVG). Bovendien moet hij nog steeds in zijn hoedanigheid van verantwoordelijke voor de gegevensverwerking alle nodige maatregelen invoeren (artikel 24 van de AVG). De Geschillenkamer benadrukt, zoals zij reeds in eerdere beslissingen tegen overheidsmandatarissen[2] heeft aangegeven, dat de overheidssector in het algemeen het goede voorbeeld moet geven in de maatregelen die zij neemt om de eerbiediging van het grondrecht op bescherming van persoonsgegevens te waarborgen.

In artikel 32 van de AVG (veiligheidsverplichting) wordt gespecificeerd:

[2] Zie Gegevensbeschermingsautoriteit, Geschillenkamer, Beslissingen 10/2019 en 11/2019 van 25 november 2019 waarin de Geschillenkamer eraan herinnert dat de hoedanigheid van overheidsmandaaris van de verwerkingsverantwoordelijke moet samengaan met een voorbeeldige houding ten aanzien van de naleving van de wetgeving, ook deze inzake persoonsgegevensbescherming.

"1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

(…)

b) het vermogen om permanent de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

(…)

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking (...)".[3].

Dit artikel 32 vertaalt artikel 5,1.f), van de AVG (hoofdstuk II-beginselen), waarin het beginsel van integriteit en vertrouwelijkheid in deze woorden wordt uiteengezet:

"Persoonsgegevens moeten: f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging".

De beveiliging van persoonsgegevens is als beginsel vastgesteld - wat het toegenomen belang ervan aantoont - aangezien deze niet was opgenomen in artikel 6 van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, die bij de inwerkingtreding van de AVG is ingetrokken).

Een van de passende veiligheidsmaatregelen om de vertrouwelijkheid van de gegevens te waarborgen, is dat een verwerkingsverantwoordelijke zoals de verweerder noodzakelijkerwijs organisatorische en technische veiligheidsmaatregelen moet treffen die een controle van de toegangen[4] garanderen: Met

---

[3] Het is de Geschillenkamer die onderlijnt.

[4] Zie met name de Referentiemaatregelen van de Commissie voor de bescherming van de persoonlijke levenssfeer voor de beveiliging van elke verwerking van persoonsgegevens, https://www.gegevensbeschermingsautoriteit.be/lexicon/referentiemaatregelen-voor-de-beveiliging-van-elke-verwerking-van-persoonsgegevens.

Logische toegangsbeveiliging

De instelling moet zich ervan vergewissen dat de persoonsgegevens overeenkomstig hun classificatie slecht toegankelijk zijn voor de personen (en toepassingsprogramma's) die hiertoe uitdrukkelijk gemachtigd zijn.

Hij zal een bijgewerkte lijst bijhouden van de verschillende personen die gemachtigd zijn om toegang te krijgen tot deze gegevens en ze te verwerken, alsook van hun respectieve bevoegdheden (creatie, raadpleging, wijziging, vernietiging).

Deze verschillende machtigingen moeten worden vertaald in technische apparaten en toegangscontroles voor de verschillende IT-elementen (programma's, procedures, opslagelementen, telecommunicatieapparatuur, etc.) die betrokken zijn bij de verwerking van persoonsgegevens.

andere woorden, alleen personen die in de uitoefening van hun eigen functie toegang tot dergelijke gegevens moeten hebben, zouden de nodige toegang moeten krijgen.

De Geschillenkamer herinnert in dit verband aan artikel 5.1.b) van de AVG (hoofdstuk II-beginselen), waarin het doelbeginsel is vastgelegd, namelijk dat gegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en niet verder mogen worden verwerkt op een wijze die onverenigbaar is met die doeleinden. In dit verband is de verweerder gemachtigd om het Rijksregister te raadplegen voor welbepaalde doeleinden overeenkomstig de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen*.

De verwerkingsverantwoordelijke dient er derhalve voor te zorgen dat de persoonsgegevens alleen toegankelijk zijn voor personen en toepassingen die daartoe uitdrukkelijk gemachtigd zijn. Elke persoon dient een eigen account te krijgen en de toegang tot persoonsgegevens dient uitsluitend te worden toegestaan op basis van het "need-to-know"-beginsel. Deze personen mogen alleen toegang hebben tot de functionaliteit of de gegevens die zij nodig hebben voor de uitvoering van hun taken en dit met inachtneming van het finaliteitsbeginsel.

In haar Aanbeveling 03/2017, waarnaar de Inspecteur-Generaal ook verwijst, heeft de toenmalige Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) verklaard dat het verantwoordingsplichtbeginsel (artikel 5.2. en 24 van de AVG) hierboven in herinnering gebracht "daarom niet alleen betekent dat de verwerkingsverantwoordelijke de bepalingen van de AVG naleeft, maar ook dat hij dit kan aantonen (...). Artikel 16 AVG herhaalt dat het niet volstaat om passende technische en organisatorische maatregelen te treffen in naleving van de Verordening; dit moet gebeuren op een transparante en traceerbare wijze die toelaat om bij een gezette controle het bewijs van de geïmplementeerde waarborgen te leveren" (punt 16 van de aanbeveling 07/2017).

Aanbeveling 01/2017 bepaalt verder dat de AVG, die toen van kracht maar nog niet van toepassing was, de bestaande verplichtingen van de WVP [lees de Privacywet, d.w.z. de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens] zal versterken, zodra deze in werking treedt op 25 mei 2018, de verantwoordelijken voor de verwerking, in dit geval de steden en gemeenten - met inbegrip van de verweerder - zal onderwerpen aan het beginsel van de verantwoordingsplicht en ook de lat met betrekking tot de transparantie van de verwerking zal verhogen (transparantiebeginsel). "Deze aanbeveling besluit: "Uit een samenlezing van de huidige nationale rechtsbepalingen en de

Deze technische voorzieningen moeten zowel upstream (applicatieontwikkeling) als downstream (back-up management) activiteiten omvatten.

Indien het veiligheidsniveau dit vereist, wordt de identificatie van de deelnemers aangevuld met een authenticatieprocedure.

toekomstige AVG besluit deze aanbeveling dat de opgave van de reden voor de raadpleging een noodzakelijke en verplichte waarborg uitmaakt die de rechtmatige toegang tot het Rijksregister omkadert. (punt 6 van de aanbeveling 07/2017)[5].

Het is derhalve aan verweerder om ervoor te zorgen dat de toegang tot het Rijksregister beperkt blijft tot de doeleinden waarvoor deze toegang is toegestaan. Het is ook aan de aanvrager om dit aan te kunnen tonen.

De naleving van het finaliteitsbeginsel, de pijler van de gegevensbescherming, kan niet worden gecontroleerd als het personeel van een structuur als de verweerder de reden voor de door hem uitgevoerde raadpleging niet vastlegt. In dit verband is het eveneens van essentieel belang dat de verweerder, overeenkomstig artikel 24 van de AVG, over een passend controlemechanisme beschikt om ervoor te zorgen dat haar gemachtigde ambtenaren het Rijksregister alleen voor die doeleinden raadplegen. De verweerder moet over een computertoepassing beschikken die het mogelijk maakt elke raadpleging door zijn personeel te legitimeren en zo aan te tonen dat de raadpleging heeft plaatsgevonden in het kader van de uitoefening van de taken van het personeelslid dat de raadpleging heeft uitgevoerd.

Naast artikel 32 van de AVG is de verweerder, in zijn hoedanigheid van de autoriteit die toegang heeft tot het Rijksregister, ook verplicht de specifieke bepalingen van de wet van 8 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen na te leven*. Dit artikel 17 van deze wet - in werking getreden op 23 december 2018 - waarnaar de Inspecteur-generaal verwijst, luidt als voglt:

> *« Elke openbare overheid, openbare of private instelling die de machtiging heeft gekregen om toegang te hebben tot de informatiegegevens van het Rijksregister van de natuurlijke personen, met inbegrip van de politiediensten, alsook de justitiediensten vermeld in de artikelen 5 en 8 moet de uitgevoerde consultaties kunnen verantwoorden, ongeacht of die uitgevoerd zijn door een individuele gebruiker of door een automatisch informaticasysteem. Daartoe houdt elke gebruiker een consultatieregister bij teneinde de traceerbaarheid van de consultaties te verzekeren.*
>
> *Dit register vermeldt de identificatie van de individuele gebruiker of van het proces of systeem dat toegang tot de gegevens heeft gehad, de gegevens die geraadpleegd werden, de wijze waarop ze geraadpleegd werden, met name voor lezing of voor wijziging, de datum en het uur van de consultatie, alsook het doeleinde waarvoor de gegevens van het Rijksregister van de natuurlijke personen geraadpleegd werden.*

[5] Het is de Geschillenkamer die onderlijnt.

(…) ».[6]

De Geschillenkamer heeft reeds aangegeven dat de feiten die aanleiding geven tot de klacht vóór 25 mei 2018 liggen en dat zij er dus geen kennis van kan nemen. Uit de inspectie - uitgevoerd van 21 november 2018 tot 17 mei 2019 - is echter gebleken dat verweerder in het algemeen de technische en organisatorische maatregelen die nodig zijn om aan artikel 5.2, 24 van de AVG te voldoen, nog niet heeft voltooid. (verantwoordingsplichtbeginsel), aslook artikel 32 van de AVG en artikel 17 van de wet van 8 augustus 1983 tot instelling van een Rijksregister van natuurlijke personen (veiligheidsverplichting), in samenhang met de artikelen 5.1.b en 5.1.f van de AVG (finaliteits- en veiligheidsbeginsel), wat de verweerder niet betwist..

VII. Over corrigerende maatregelen en sancties

Krachtens artikel 100 WOG, heeft de Geschillenkamer de bevoegdheid om:
1° een klacht te seponeren;
2° de buitenvervolgingstelling te bevelen;
3° een opschorting van de uitspraak;
4° een schikking voor te stellen;
5° waarschuwingen en berispingen te formuleren;
6° te bevelen dat wordt voldaan aan de verzoeken van de betrokkene om zijn rechten uit te oefenen;
7° te bevelen dat de betrokkene in kennis wordt gesteld van het veiligheidsprobleem;
8° te bevelen dat de verwerking tijdelijk of definitief wordt bevroren, beperkt of verboden;
9° te bevelen dat de verwerking in overeenstemming wordt gebracht;
10° de rechtzetting, de beperking of de verwijdering van gegevens en de kennisgeving ervan aan de ontvangers van de gegevens te bevelen;
11° de intrekking van de erkenning van certificatie-instellingen te bevelen;
12° dwangsommen op te leggen;
13° administratieve geldboeten op te leggen;
14° de opschorting van grensoverschrijdende gegevensstromen naar een andere Staat of een internationale instelling te bevelen;
15° het dossier over te dragen aan het parket van de procureur des Konings te Brussel, die het in kennis stelt van het gevolg dat aan het dossier wordt gegeven;
16° geval per geval te beslissen om haar beslissingen bekend te maken op de website van de Gegevensbeschermingsautoriteit.

[6] Het is de Geschillenkamer die onderlijnt.

Het is belangrijk om de niet-naleving van de artikelen 5.2. en 24 van de AVG, alsook de artikelen 32 van de AVG en 17 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, in combinatie met de artikelen 5 § 1 b) en f) van de AVG, in zijn context te plaatsen om de meest geschikte corrigerende maatregelen vast te stellen.

De Geschillenkamer merkt op dat zowel het veiligheidsbeginsel (artikel 5, § 1, f) van de AVG) (en de daaruit voortvloeiende verplichtingen - artikel 32 van de AVG) als het finaliteitsbeginsel (artikel 5, § 1, b) van de AVG), dat het veiligheidsbeginsel garandeert, de wezenlijke beginselen zijn van het beschermingsstelsel dat door de AVG is vastgesteld. Het in artikel 5.2. van de AVG vastgelegde en in artikel 24 verder uitgewerkt beginsel van de verantwoordingsplicht, vormt de kern van de AVG en weerspiegelt de paradigmaverschuiving die de AVG teweegbrengt, van een regeling die gebaseerd is op voorafgaande aangiftes en machtigingen van de toezichthoudende autoriteit naar een grotere verantwoordingsplicht en verantwoordelijkheid van de verwerkingsverantwoordelijke. Dit maakt het des te belangrijker dat deze laatste aan zijn verplichtingen voldoet en dit kan aantonen. Schendingen van deze beginselen vormen ernstige inbreuken.

Wat het aantal potentieel betrokken personen betreft, omvat het Rijksregister een identificatiegegevensbank van *alle* natuurlijke personen die zijn ingeschreven in het bevolkingsregister, het wachtregister en het vreemdelingenregister die worden bijgehouden door de gemeenten of de consulaire registers, d.w.z. voor de verweerder alleen al, meer dan XXX ingeschrevenen op een totaal van 11 miljoen personen die in het Rijksregister zijn ingeschreven.

De omvang van de handelingen die steden en gemeenten, zoals de verweerder in het Rijksregister verrichten, kan bovendien geen afbreuk doen aan de verplichting om te voorzien in een mechanisme dat de naleving waarorgt van de doeleinden waarvoor de gegevens in het Rijksregister toegankelijk zijn, via de vermelding van de reden voor die toegang noch aan het vereiste van een effectieve controle. Integendeel, zowel artikel 32 als artikel 24 van de AVG schrijven voor dat de aard van de technische en organisatorische maatregelen die een gemeente treft in verhouding staat tot de ernst van de risico's voor de rechten en vrijheden van de betrokken personen. Deze databank, die een bepaalde hoeveelheid informatie bevat - zij het beperkt - over meer dan 11 miljoen personen, vereist van nature een bijzonder streng toezicht, niet alleen vanwege de omvang ervan, maar ook vanwege het doel om informatie over de identificatie van natuurlijke personen vast te leggen, op te slaan en door te geven.

De Geschillenkamer merkt op dat het Sectoraal Comité van het Rijksregister in 2015 bijkomende duiding gaf bij de precieze omvang van deze plicht tot het houden van logbestanden in het kader van de toegang tot het Rijksregister door lokale besturen. In deze Aanbeveling verduidelijkt het Comité *"Deze logging moet tevens de identificatie bevatten van de individuele gebruiker of van het proces of*

het systeem dat toegang had tot de gegevens, welke gegevens werden geraadpleegd, de wijze waarop de toegang plaatsvond (raadpleging, wijziging, enz.), wanneer de toegang plaatsvond, alsook de reden hiervoor".[7] Het Comité beval ook aan om daarnaast te voorzien in een verplicht veld voor de registratie van de reden van de toegang.

De Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) had ook al vóór Aanbeveling 01/2017 herhaaldelijk aangegeven dat de registratie van de reden voor het raadplegen van het Rijksregister van cruciaal belang was.[8]

Het is waar, het betrof hier aanbeveligen. Deze aanbevelingen om een dergelijk mechanisme in te voeren weerspiegelen echter de grote bezorgdheid die lang voor de inwerkingtreding van de AVG, al bestond Met andere woorden, de kwesite was niet nieuw en de verweerder kon deze op grond van zijn hoedanigheid niet negeren.

De Geschillenkamer stelt ook vast dat de verweerder, zowel tijdens de inspectie als in zijn conclusies, verschillende beslissingen heeft genomen om te voldoen aan zijn veiligheidsverplichtingen en de vereisten van de AVG en de wet van 3 augustus 1983 *tot regeling van een Rijksregister van de natuurlijke personen.* Deze beslissingen blijken uit verschillende documenten in het dossier, zoals interne documentatie over de toegang tot het Rijksregister, de benoeming en het werk van de functionaris voor gegevensbescherming (advies van 5 april 2019) en een aanbeveling van 25 april 2019 (aanvaard op 6 mei 2019) om de reden voor de raadpleging verplicht te stellen waarvan de implementatie werd voorzien tegen het laatste kwartaal van 2019[9]. De Geschillenkamer merkt op dat deze documenten en beslissingen voor het grootste deel zijn aangenomen tijdens de inspectie.

Bovendien blijkt uit de documenten die de verweerder heeft ingediend in het kader van de opvolging waartoe de Geschillenkamer na de hoorzitting van 18 november 2019 heeft besloten, dat de werkzaamheden voor de tenuitvoerlegging van de aanbeveling van de DPO om het doeleinde waarvoor de gebruiker de gegevens in het Rijksregister raadpleegt (naast de andere gegevens die overeenkomstig artikel 17 van de Rijksregisterwet van 8 augustus 1983 moeten worden geregistreerd) in het laatste kwartaal van 2019 daadwerkelijk werd voortgezet (notulen van de vergadering "Toegang tot het Rijksregister van 16 september 2019 ").

---

[7] Aanbeveling 01/2015 van het Sectoraal Comité van het Rijksregister aan de gemeenten en lokale besturen betreffende de informatiebeveiliging waarmee de toegangen tot het Rijksregister en de daaruit volgende verwerkingen van Rijksregistergegevens moeten worden omkaderd, 18 februari 2015, Randnummers 44-49.

[8] Zie punt 23 van de Aanbeveling 01/2017 reeds eerder vermeld en de genoemde referenties.

[9] Zie het stuk "vergadering toegang tot het Rijksregister van 3 mei 2019" van de verweerder.

Uit de documenten in het dossier blijkt ook dat de DPO van de verweerder aanbevelingen heeft gedaan met betrekking tot de *controle* op de toegangen tot het Rijksregister (uittreksel uit de notulen van de vergadering "Toegang tot het Rijksregister van 16 september 2019 ").

De Geschillenkamer stelt ook vast dat de follow-up van de aanbevelingen van de DPO in de loop van oktober 2019 met name heeft geresulteerd in de vaststelling van de redenen voor raadpleging voor elk van de groepen die toegang hebben tot het Rijskregister en de invoering daarvan in "SAPHIR ".

De Geschillenkamer stelt eveneens vast dat per e-mail van 22 november 2019 met als titel : "Belangrijk AVG SAPHIR - Raadpleging RR : nieuwe procedure", door de verweerder werd verstuurd aan zijn peronseelsleden, waarbij zijn DPO hen inlicht dat een procedure is ingevoerd waarbij voortaan elke raadpleging betreffende een burger in het Rijskregister moet voorafgaan met het kiezen van een reden voor de raadpleging. In de Saphir-toepassing zal bij elk verzoek om raadpleging van het Rijksregister van de personeelsleden een keuzelijst verschijnen met een reeks redenen voor raadpleging die verband houden met hun respectievelijke bevoegdheden. Tijdens deze procedures, zal het personeel een doeleinde moeten selecteren dat overeenstemt met het soort dossier dat zij behandelen.

De Geschillenkamer merkt voorts op dat verweerder per e-mail van dezelfde 22 november 2019 aan zijn IT-correspondenten een bericht heeft doen toekomen volgens hetwelk een periodieke (driemaandelijkse) en systematische controle van de verleende toegang is ingevoerd: een lijst met de naam, de voornaam en de bijbehorende toegangsgroep voor elke ambtenaar die in de databank " Users Saphir - RN " is opgenomen. De controle zal vragen om een bevestiging van de namen van de ambtenaren voor wie de toegang moet behouden blijven. Zonder antwoord, zullen de toegangen systematische worden opgeheven.

Naast deze specifieke maatregelen met betrekking tot het vermelden van de reden voor het raadplegen van het Rijksregister, heeft de verweerder het opleidingsmateriaal dat wordt gebruikt ter ondersteuning van interne sessies om de AVG onder de aandacht te brengen, aan de Geschillenkamer toegezonden. Hij heeft de Geschillenkamer ook op de hoogte gebracht van de uitwisseling van e-mails tussen zijn DPO en zijn verschillende departementsverantwoordelijken met betrekking tot de voltooiing van de registers van de verwerkingsactiviteiten (artikel 30.1 van de AVG) en de ook de Registers zelf van de verwerkingsactiviteiten van de verschillende departementen. Verweerder stelt dat de opstelling van deze registers ook voor de overige departementen staat ingepland.

De Geschillenkamer neemt nota van deze informatie en van de documenten die haar worden toegezonden. Zij is van mening dat deze documenten het bewijs vormen van een aantal stappen die de verweerder heeft ondernomen om aan zijn verplichtingen als verantwoordelijke voor de verwerking te voldoen. Hoewel de Geschillenkamer dergelijke stappen toejuicht, betreurt het echter dat de

verweerder, die zich bewust is van zijn veiligheidsverplichtingen, niet van zijn ambtenaren heeft geëist dat zij in afwachting van geautomatiseerde oplossingen een handmatige registratie van de toegangen en de redenen daarvoor bijhouden.

In het algemeen onderstreept de Geschillenkamer de goede samenwerking van de verweerder - wat wordt vereist door artikel 31 van de AVG - zowel met de Inspecteur-generaal als met de Geschillenkamer.

In het licht van de hierboven uiteengezette elementen, eigen aan dit dossier, is de Geschillenkamer van mening dat de vastgestelde feiten en de inbreuk - die volgens de verweerder inmiddels is verholpen - op artikel 5.2. en 24 van de AVG, artikel 32 van de AVG en artikel 17 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, in samenhang met artikel 5, § 1, b) en f) van de AVG , rechtvaardigen dat als een doeltreffende, evenredige en afschrikkende sanctie (artikel 100, §1 , 5° van de WOG) aan verweerder een berisping wordt opgelegd.

Gezien het belang van transparantie met betrekking tot het besluitvormingsproces en de beslissingen van de Geschillenkamer zal dit besluit worden gepubliceerd op de website van de Gegevensbeschermingsautoriteit, waarbij de directe identificatiegegevens van de genoemde partijen en personen zullen worden verwijderd.

OM DEZE REDENEN,
DE GESCHILLENKAMER,

Beslist, na beraadslaging, om de verweerder een berisping op te leggen op grond van artikel 100 § 1, 5° van de WOG.

*

Tegen deze beslissing kan op grond van art. 108, §1 WOG, beroep worden aangetekend binnen een termijn van dertig dagen, vanaf de betekening van de kennisgeving, bij het Marktenhof, met de Gegevensbeschermingsautoriteit als verweerder.

(get.) Hielke Hijmans
Voorzitter van de Geschillenkamer