AUTORITEIT
PERSOONSGEGEVENS

**Autoriteit Persoonsgegevens**
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Het College van burgemeester en wethouders
van de gemeente Eindhoven
Postbus 90150
5600 RB Eindhoven

Datum
17 april 2024

Ons kenmerk
z2022-04286

Contactpersoon

Onderwerp
Beoordeling ingediende stukken en uitnodiging voor gesprek

Geacht college,

Bij brief van 1 maart 2023 heeft de Autoriteit Persoonsgegevens (hierna: AP) het toezicht op uw college geïntensiveerd. In het kader van dit geïntensiveerde toezicht heeft de AP vijf indicatoren vastgesteld. Te weten: 1) bewaartermijnen, 2) DPIA's, 3) datalekken, 4) positie en rol van de FG en 5) governance en organisatiecultuur. U heeft in dit kader op 28 april 2023 en op 30 december 2023 verschillende documenten ingediend.

## Beoordeling ingediende stukken en uitnodiging wethouder en burgemeester voor gesprek.

De AP dankt het college van de gemeente Eindhoven voor de op 30 december 2023 ingediende documenten in het kader van het geïntensiveerde toezicht op de gemeente Eindhoven. De AP heeft de documenten beoordeeld en zal in het vervolg van deze brief haar constateringen nader uiteenzetten. De AP wil benadrukken dat het met deze brief dus reageert op de situatie van ruim vier maanden geleden. De AP beseft zich terdege dat de huidige situatie mogelijk anders is dan die van vier maanden geleden. Toch acht de AP het wenselijk alsnog de beoordeling van de ingediende stukken via deze weg met u te delen.

De AP heeft daarnaast het afgelopen half jaar meerdere vertrouwelijke signalen over mogelijke schendingen van de privacyregels door de gemeente Eindhoven ontvangen. De constateringen en de vertrouwelijke signalen zijn voor de AP aanleiding om de verantwoordelijk wethouder en de burgemeester van de gemeente Eindhoven uit te nodigen voor een gesprek.

Datum
17 april 2024

Ons kenmerk
z2022-04286

## Samenvattende constateringen

De AP constateert dat het college aan de gemeenteraad heeft aangegeven voorrang te geven aan de implementatie van het verbeterplan en zeer terughoudend is ten aanzien van een snelle invoering van een nieuwe stadspas als gevolg van de privacyrisico's. Daarnaast heeft het college verschillende (externe) onderzoeken laten uitvoeren en erkent het college dat de privacy- en informatiehuishouding van de gemeente op dit moment op volwassenheidsniveau 1 (op een schaal van 0 tot 5, waarbij 5 het hoogst haalbare is) functioneert. De AP constateert daarnaast dat de ambitie van het college hoog is. Het college wil niet alleen aan de AVG voldoen, maar streeft op langere termijn zelfs naar certificering.
Het is goed om te zien dat het college erkent dat het huidige volwassenheidsniveau van de informatie- en privacyorganisatie niet voldoende is en dat het college ambitieus is in haar doelstelling voor de toekomst.

De AP constateert echter ook dat het college de zorgen van de AP over het niet voldoende naleven van de AVG nog onvoldoende heeft kunnen wegnemen. Zo is het voor de AP nog onvoldoende duidelijk hoe en wanneer het college de benodigde verbeteringen denkt te kunnen hebben doorgevoerd. Ook is niet duidelijk hoeveel capaciteit het college daarvoor nodig denkt te hebben en of die capaciteit dan ook gerealiseerd gaat worden. De AP wijst er op dat de FG en het externe bureau Lex Digitalis hierover ook expliciet hun zorgen uitspreken. De AP deelt voorts de zorgen van de FG over de haalbaarheid van het opgestelde verbeterplan, als ook de zorgen over het huidige volwassenheidsniveau van de organisatie in combinatie met het datagedreven werken binnen de gemeente Eindhoven.
In het verbeterplan van het college wordt aangegeven: "in het nieuwe jaar [wordt] gestart met een onderzoek met als doel het bepalen waar de gap zit tussen de huidige beschikbare, de gewenste en benodigde capaciteit in kennis en middelen." De AP maakt hieruit op dat ook bij het college zelf op dit moment nog onvoldoende zicht is op wanneer de benodigde verbeteringen bewerkstelligd kunnen worden, omdat nog niet helder is waar het op dit moment binnen de organisatie aan schort.

De AP acht het noodzakelijk dat er binnen een half jaar, aldus voor 1 juli, een duidelijke concretisering plaatsvindt in de doelen en de tijdsplanning daarvan. Indien het college de geconstateerde zorgen ook na deze periode onvoldoende heeft weggenomen dan dient het college er rekening mee te houden dat de AP mogelijk andere handhavingsmiddelen zal inzetten.

In het vervolg van deze brief worden, per indicator, enkele opvallende zaken besproken die hebben geleid tot het oordeel van de AP dat verlenging van het geïntensiveerde toezicht op dit moment nog benodigd is. Deze opsomming is niet uitputtend bedoeld.

## 1. Bewaartermijnen

De systemen waarbinnen de bewaartermijnen niet (kunnen) worden nagekomen, omvatten verschillende processen waaronder ook gegevensverwerkingen die complex en veelomvattend zijn. In deze grote processen vinden ook verwerkingen met bijzondere persoonsgegevens plaats. Het betreft hier: gegevens uit het sociaal domein; gegevens die nodig zijn bij het innen van belastingen (zelfs tot en met bezwaar en beroep); processen rondom APV-vergunningen, en processen aangaande de burgerlijke stand.

Uit de ingediende informatie over het project Herstel werkzaamheden Document Management Systeem eDocs blijkt dat al geruime tijd bij het college bekend was dat bewaartermijnen niet kunnen worden nagekomen. Het besluit om over te gaan naar een ander systeem is al eind 2016 genomen. Daarnaast constateert de AP, na bestudering van de door het college aangeleverde stukken, dat het probleem rond het nakomen van de bewaartermijnen niet in 2024 kan worden opgelost, maar zeker nog tot 2025 zal voortduren. Uit de overlegde stukken blijkt dat dit het gevolg is van een combinatie van technische (on)mogelijkheden en een gebrek aan beschikbare capaciteit.

## 2. DPIA's

### Verwerkingsregister

In het opgestelde verbeterplan geeft het college aan dat het verwerkingsregister niet actueel en juist is. Het is zeer goed mogelijk dat dit gevolgen heeft voor de volledigheid van het overzicht van verwerkingen waarvoor een Data Protection Impact Assessment (DPIA) moet worden uitgevoerd. Immers, indien de informatie over de verwerkingen niet volledig en actueel is, kan dit gevolgen hebben voor het overzicht van de DPIA's die moeten worden uitgevoerd (onvolledig) of het juist uitvoeren van DPIA's.

### Overkoepelende DPIA's

Daarnaast valt het de AP op dat in het verbeterplan staat dat wordt onderzocht of overkoepelende DPIA's uitgevoerd kunnen worden, waarbij verwerkingen worden gecategoriseerd en dan voor vergelijkbare verwerkingen een overkoepelende DPIA wordt uitgevoerd. De AP benadrukt dat de AVG voorschrijft dat de DPIA-plicht geldt voor een verwerking met een waarschijnlijk hoog risico voor de privacy van betrokkenen. Het uitvoeren van overkoepelende DPIA's lijkt dan ook moeilijk verenigbaar met de AVG.

### Maatregel in verbeterplan onduidelijk

In het verbeterplan is bij de maatregel: "Geen risicovolle verwerking starten zonder afronding DPIA", het volgende opgenomen: "Afgerond betekent dat de maatregelen bepaald in de planning uitvoering maatregelen geïmplementeerd zijn. Dit punt is tevens onderdeel van sturing en de PDCA"

Het is onduidelijk of het college er hiermee van uitgaat dat de maatregelen in een planning bepaald moeten worden of dat de maatregelen geïmplementeerd moeten zijn voordat de verwerking kan worden gestart. Dit zou duidelijker geformuleerd moeten worden.

## 3. Datalekken

In 2022 heeft het FG-bureau onderzoek gedaan naar de registratie en meldplicht van datalekken door het college. Dit onderzoek heeft een langere doorlooptijd gekend als gevolg van het traject van de organisatie met de AP. De bevindingen en aanbevelingen zijn volgens de FG desalniettemin nog steeds actueel. De resultaten en aanbevelingen uit het FG-onderzoek zijn bij besluit van 24 oktober 2023 overgenomen door het college. In dit onderzoek zijn de volgende bevindingen opgenomen:

Bevindingen met betrekking tot de datalekkenregistratie

- In opzet is er sprake van volledigheid van het datalekkenregister.
- In de registratie wordt niet consistent en volledig gerapporteerd.
- In dat kader is tevens naar voren gekomen dat het op inactief plaatsen van datalekregistraties nog om aandacht vraagt, alsook het moment waarop dit gebeurt en of dit besluit expliciet wordt genomen door degene die daarvoor de verantwoordelijkheid draagt.

Bevindingen met betrekking tot het informeren van betrokkenen

- Betrokkenen worden in veel gevallen niet afdoende en adequaat geïnformeerd over een datalek.
- Omdat kaders ontbreken worden definities niet eenduidig gehanteerd waardoor soms de verkeerde persoon wordt geïnformeerd over een datalek.
- Bij het informeren van betrokkenen wordt niet altijd gecommuniceerd of het datalek daadwerkelijk gedicht is waardoor het voor betrokkene niet duidelijk is wat de eventuele gevolgen kunnen zijn.
- Tijdigheid van het informeren van betrokkenen (zo snel mogelijk na het optreden van het datalek) is een aandachtspunt.
- De geregistreerde inhoud van de mondelinge informatieverstrekking is niet toetsbaar aan de vereisten vanuit de AVG wegens het ontbreken van een schriftelijke bevestiging van de gegeven informatie.
- Te zien is dat de keuze voor de informatie die aan betrokkene wordt verstrekt nog vooral wordt aangevlogen vanuit het belang van de organisatie in plaats vanuit het belang van betrokkene.

Bevindingen met betrekking tot AP-meldingen

- Er blijft sprake van te late meldingen aan de AP.
- De inhoud van de AP-meldingen komt niet overeen met de informatie in het register.
- Uit het onderzoek blijkt niet dat het besluit tot het al dan niet melden bij de AP genomen wordt door de eerstelijns verwerkingsverantwoordelijke.

## 4. Positie en rol FG

In het verbeterplan staan enkele zaken opgenomen die niet passen bij de onafhankelijke toezichthoudende rol van de FG. Zo zijn in bijlage C van het verbeterplan de volgende zaken te lezen die niet stroken met de onafhankelijke rol van de FG:

- Richting en sturing geven aan het algehele programma, zodat gewaarborgd wordt dat het programma 'levensvatbaar' blijft en binnen eventueel gestelde randvoorwaarden
- [De FG] is beslissingsbevoegd m.b.t. het nemen van besluiten m.b.t. het evt. afwijken van de scope van het VBP 2.0 en over geëscaleerde issues.

De AP is van oordeel dat de FG de toezichthoudende taken die in de AVG benoemd worden onafhankelijk moet kunnen uitvoeren. Dit moet door het college geborgd worden.

## 5. Governance en organisatiecultuur

De AP constateert dat de cultuurscan (nulmeting mei 2023) zich met name heeft gericht op informatiebeveiligingsaspecten en dat overige privacyzaken maar marginaal aan bod komen. Ook heeft maar 31,8% van de medewerkers (768 van de 2418) meegewerkt aan de cultuurscan. Het is dan ook de vraag in hoeverre deze cultuurscan nu daadwerkelijk bruikbaar is.

De AP wijst voorts ook op de volgende bevindingen uit het onderzoek van Lex digitalis van 9 december 2023:

- Sectoren zijn onvoldoende gemotiveerd en in staat zelf het privacyrecht toe te passen
- Privacy officers komen niet toe aan hun controlerende en bewakende taak
  (o.a. de privacy juridische kennis bij de privacy officers is beperkt, voor de gehele gemeentelijke organisatie is sinds kort één privacyjurist beschikbaar.)
- FG komt onvoldoende toe aan het uitoefenen van de kerntaken van de derde lijn

Wat de AP betreft zijn dit stuk voor stuk zorgwekkende bevindingen.

## Geïntensiveerd toezicht

Uw college dient, zoals eerder afgesproken, **uiterlijk 1 juli 2024** opnieuw een rapportage over de voortgang van de vijf vastgestelde indicatoren bij de AP in te dienen. De AP verwacht daarnaast dat het verbeterplan wordt aangepast op basis van de benoemde constateringen van de AP.

Ten overvloede wordt opgemerkt dat de AP op elk moment in het proces kan besluiten om ook andere (handhavings)instrumenten in te zetten, als daar aanleiding toe is.

## Uitnodiging voor gesprek

De AP verwacht de verantwoordelijke wethouder en de burgemeester ten kantore van de AP om uitleg te geven over de huidige stand van zaken. De AP zal hiervoor een afspraak in het tweede kwartaal van dit jaar inplannen. Wij verzoeken u om uw FG bij dit overleg te laten aansluiten. De AP zal voor het plannen van de afspraak contact opnemen met uw secretariaat.

Een afschrift van deze brief zal ook met uw FG worden gedeeld.

Hoogachtend,
Autoriteit Persoonsgegevens,

ir. M.J. Verdier
vicevoorzitter