

**Aan de leden van Provinciale Staten van Noord-Holland****Datum ingekomen vragen** : 28 februari 2020**Datum GS-besluit** : 14 april 2020**Vragen nr. 19**Vragen van de heer **J.J. Carton** (PvdA) over Bescherming persoonsgegevens

De voorzitter van Provinciale Staten van Noord-Holland deelt u overeenkomstig het bepaalde in artikel 45 van het Reglement van Orde voor de vergaderingen en andere werkzaamheden van Provinciale Staten mede, dat op 28 februari 2020 door het lid van Provinciale Staten, de heer **J.J. Carton** (PvdA), de volgende vragen bij Gedeputeerde Staten zijn ingekomen.

**INLEIDING VRAGEN**

De PvdA vindt het belangrijk dat de provincie uiterst zorgvuldig en veilig met de persoonsgegevens van de inwoners om gaat.

De provincie verwerkt veel (gevoelige) persoonsgegevens van de inwoners van de provincie. En met de verdergaande digitalisering (denk bijv. aan Smart Mobility) zal dit nog meer worden. In de privacyverklaring van de provincie verklaart de provincie daarom terecht: 'Om uw recht op privacy te waarborgen gaat de provincie uiterst zorgvuldig en vertrouwelijk om met uw persoonsgegevens. Uiteraard houdt de provincie zich aan de Algemene Verordening Gegevensbescherming (AVG).'<sup>1</sup>

Volgens het nieuwsbericht van de Autoriteit Persoonsgegevens (AP) op 6 februari jl. ontving de AP in 2019 4.624 datalekmeldingen uit de sector openbaar bestuur. Dit zijn 27% meer meldingen dan in 2018. Verder geeft de AP aan dat het de komende jaren in het toezichtwerk extra nadruk op een aantal focusgebieden waaronder de digitale overheid. Centrale en lokale overheden beschikken over een grote hoeveelheid - vaak gevoelige en bijzondere - persoonsgegevens, zoals Burgerservicenummers en gegevens over zorg en maatschappelijke dienstverlening. Het gaat met name om wettelijke en/of onvrijwillige verwerking van gegevens

---

<sup>1</sup> [https://www.noord-holland.nl/Configuratie/Terugkerende\\_navigatie/Privacyverklaring](https://www.noord-holland.nl/Configuratie/Terugkerende_navigatie/Privacyverklaring)

en burgers kunnen niet terecht bij een alternatieve dienstverlener. Datalekken in deze sector kunnen daarom grote impact hebben op burgers. <sup>2</sup>

Er is dus sprake van toenemende digitalisering en datalekken en een extra nadruk komende jaren van de Autoriteit Persoonsgegevens te verwachten op de digitale overheid van lokale overheden.

---

2

[https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarcijfers\\_meldplicht\\_datalekken\\_2019.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarcijfers_meldplicht_datalekken_2019.pdf)

Wij willen het College daarom het volgende vragen:

## **VRAGEN**

### **Vraag 1:**

Heeft de provincie een verwerkingsregister (een overzicht van alle verwerkingen van persoonsgegevens binnen de provincie)? Hoeveel verwerkingen betreft het?

### **Antwoord 1:**

Ja, de provincie beschikt over een register van de verwerkingsactiviteiten ex artikel 30 van de Algemene verordening gegevensbescherming (AVG). Er staan 134 processen in waarbij persoonsgegevens worden verwerkt.

### **Vraag 2:**

Hoeveel verwerkingen zijn zgn. risicovolle verwerkingen, waarvoor volgens de Algemene Verordening Gegevensbescherming een Data Privacy Impact Assessment (DPIA) verplicht is?

### **Antwoord 2:**

De Autoriteit Persoonsgegevens maakt een onderscheid tussen bestaande verwerkingen en nieuwe verwerkingen.

Voor een bestaande verwerking is het soms nodig alsnog een data protection impact assessment (DPIA) uit te voeren. Dat is nodig als er sprake is van een verandering van het risico van de gegevensverwerking en de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

Van de reeds bestaande verwerkingen zijn geen DPIA's gemaakt (zie antwoord vraag 3).

Van nieuwe verwerkingen zijn 2 DPIA's opgesteld (zie antwoord vraag 4).

### **Vraag 3:**

Hoeveel DPIA's van de *bestaande* verwerkingen zijn inmiddels afgerond?

### **Antwoord 3:**

Bestaande verwerkingen zijn niet veranderd op een wijze dat een DPIA noodzakelijk is. Er zijn dan ook geen DPIA's gemaakt.

### **Vraag 4:**

Hoeveel DPIA's voor nieuwe verwerkingen (die nog niet gestart zijn) heeft de provincie in 2018 en 2019 afgerond?

### **Antwoord 4:**

Twee.

### **Vraag 5:**

Kan het College aangeven in hoeveel gevallen de uit de DPIA's voortvloeiende te nemen risicobeperkende maatregelen ook zijn genomen?

### **Antwoord 5:**

Nadat de risico's in kaart zijn gebracht worden er mitigerende maatregelen voorgesteld. Deze maatregelen worden vervolgens uitgevoerd door de proceseigenaar. Van één afgeronde DPIA zijn de risicobeperkende maatregelen reeds uitgevoerd. In overleg met de softwareleverancier heeft er een aanpassing van de invulvelden plaatsgevonden.

**Vraag 6:**

Zijn er verwerkingen waarvan de Functionaris Gegevensbescherming van de provincie een negatief advies heeft gegeven met betrekking tot de verwerking? En als dat het geval is, kan het college aangeven wat de reden hiervoor is?

**Antwoord 6:**

Er is geen negatief advies uitgebracht door de Functionaris Gegevensbescherming.

**Vraag 7:**

Hoeveel datalekken heeft de provincie in 2018 en 2019 gehad? Kan het College dit specificeren naar type?

**Antwoord 7:**

In 2018 zijn 4 Datalekken gemeld bij de Autoriteit Persoonsgegevens (AP).

In 3 gevallen zijn er persoonsgegevens naar een verkeerde ontvanger verzonden. Er is meteen actie ondernomen richting de ontvanger om de gevolgen te beperken.

In 1 geval ging het om het drukken op een link in een phishing mail. Er zijn meteen technische maatregelen genomen om schade te voorkomen.

In 2019 zijn er 3 Datalekken gemeld bij de AP. In twee gevallen zijn er onterecht persoonsgegevens op een website terechtgekomen. Er is meteen actie ondernomen om deze persoonsgegevens van de website te laten verwijderen. In een geval is een tas met daarin persoonsgegevens per ongeluk achtergelaten, maar ook weer teruggegeven aan de betreffende ambtenaar.

**Vraag 8:**

In hoeveel van die gevallen heeft dat geleid tot een melding bij de Autoriteit Persoonsgegevens?

**Antwoord 8:**

Zie antwoord vraag 7.

**Vraag 9:**

Kan het College of, hoe en wanneer het privacy beleid geëvalueerd wordt, wanneer dat voor het laatst gedaan is/weer gedaan wordt en kan Provinciale Staten het verslag ontvangen?

**Antwoord 9:**

Het beleid bestaat uit verschillende protocollen.

In samenspraak met de ondernemingsraad zijn de volgende protocollen vastgesteld:

- Privacyprotocol ICT-middelengebruik 2019;
- Privacyprotocol ritregistratie 2019;
- Privacyprotocol ritregistratie, toegang en beveiliging 2019;

Tevens is er een protocol datalekken (eind 2018 gewijzigd) en een protocol voor het afhandelen van de rechten van betrokkenen (2018).

De protocollen worden aangepast indien de Algemene verordening gegevensbescherming of de Uitvoeringswet algemene verordening gegevensbescherming worden gewijzigd, dan wel informatie van de Autoriteit Persoonsgegevens of de jurisprudentie daar aanleiding voor geeft. Daar is nog geen aanleiding voor geweest. Van een dergelijke aanpassing wordt geen verslag gemaakt, dat is ook niet gebruikelijk.