AUTORITEIT
PERSOONSGEGEVENS

Toezichtkader Autoriteit Persoonsgegevens

Uitgangspunten voor toezicht 2018-2019

Den Haag, mei 2018

1. Inleiding

1.1 Naar een toekomstbestendige bescherming van persoonsgegevens

We leven in een 'datagedreven' wereld waarin data verwerkende bedrijven zeer machtige bedrijven zijn, waarin persoonsgegevens veel geld waard zijn en waarin big data-analyses in alle sectoren worden toegepast. Technologische ontwikkelingen gaan sneller dan ooit. Daarvan kan iedereen profiteren. Bedrijven en overheden, maar zeker ook de mensen die gebruik kunnen maken van nieuwe producten en diensten. Het beschermen van persoonsgegevens is essentieel in een tijd van voortdurende technologische ontwikkeling en toenemende afhankelijkheid van digitale dienstverlening. Globalisering maakt bovendien dat de verwerking van persoonsgegevens verder gaat dan de Nederlandse grenzen. In deze maatschappelijke context is het van groot belang dat mensen zeggenschap houden over hun persoonsgegevens.

Overheden en bedrijven verwerken persoonsgegevens die op steeds nieuwe manieren met elkaar worden gecombineerd. Vaak zonder dat mensen dat in de gaten hebben. Zij ondervinden gemak van innovatieve producten en diensten. Maar innovatie mag niet ten koste gaan van het grondrecht om persoonsgegevens te (kunnen) beschermen. Daarvoor is noodzakelijk dat mensen zeggenschap hebben en houden over hun digitale sporen. Dit is in deze tijd een grote uitdaging, maar alleen dan kunnen mensen in vrijheid blijven beslissen.

Vanaf 25 mei 2018 is de nieuwe Europese privacywetgeving van toepassing: de Algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming opsporing en vervolging (van '*criminal offences*'). De nieuwe wetgeving brengt ingrijpende veranderingen voor de bescherming van persoonsgegevens met zich mee, ook voor het toezicht en de toezichthouder. Deze wetgeving versterkt de privacyrechten van alle inwoners in de EU, eist meer van organisaties en geeft de Europese privacytoezichthouders steviger bevoegdheden om op te treden. Om goed uitvoering te kunnen geven aan deze nieuwe wetgeving, heeft de Autoriteit Persoonsgegevens (AP) haar interne organisatie aangepast. Bij deze vernieuwing past ook de vernieuwing van het toezichtkader.

In het voorliggende toezichtkader kunt u lezen wat de missie is van de AP, welke ambities wij hebben, volgens welke kernwaarden wij invulling geven aan de uitvoering van onze taken en welke gebieden in het bijzonder onze aandacht krijgen.

1.2 Missie

Onze wettelijke opdracht hebben wij in de volgende missie vertaald:

> De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

De AP **bevordert** dat overheden en bedrijven, maar ook mensen zelf hun verantwoordelijkheid nemen bij de bescherming van hun persoonsgegevens. Dit doen wij door hen te informeren over de regels en de risico's. Wij leggen mensen uit wat hun rechten zijn en adviseren de wetgever zowel gevraagd als ongevraagd over wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens. Daarnaast

stimuleren wij organisaties om privacyvriendelijke systemen en processen toe te passen. Wij **bewaken** naleving van de regels door onafhankelijk onderzoek te doen naar (mogelijke) overtredingen. Dat doen wij op eigen initiatief of naar aanleiding van een klacht. Als dat nodig is, treden wij handhavend op.
Wij werken samen met andere Europese privacytoezichthouders, want wij moeten reageren op nationale én internationale ontwikkelingen. Inherent daaraan is dat wij keuzes moeten maken. Keuzes over onze rol en over de meest effectieve aanpak per situatie. Bij die afweging staan altijd mensen centraal: in welke mate is hun grondrecht geschonden?

1.3 Ambities

De AP heeft drie ambities geformuleerd waarmee zij nader invulling geeft aan het volbrengen van de missie.

1. De Autoriteit Persoonsgegevens maakt zich sterk voor de bescherming van persoonsgegevens als vanzelfsprekende waarde in onze maatschappij

De AP bevordert dat een hoog privacybeschermingsniveau als vanzelfsprekend wordt beschouwd. Meer concreet beogen wij het publieke debat over de bescherming van het grondrecht op gegevensbescherming te stimuleren. Hiertoe werken wij samen en treden wij in dialoog met stakeholders om problemen en risico's te signaleren, te bespreken en waar mogelijk oplossingen aan te dragen. Daarnaast zetten wij relevante onderwerpen op de publieke agenda en communiceren wij actief over de afhandeling van klachten, alsmede over wetgevingsadviezen en besluiten.

2. De Autoriteit Persoonsgegevens kent de relevante ontwikkelingen en handelt proactief als de bescherming van persoonsgegevens in de knel komt

De AP is een kennisgedreven en risicogerichte autoriteit die in nauwe verbinding staat met haar omgeving. Wij treden actief in contact met organisaties en mensen, nemen deel aan het maatschappelijk debat en weten wat er leeft in de maatschappij. Door contact met (branche)organisaties, overheden en bedrijven halen wij kennis van buiten naar binnen en vice versa. Door middel van dienstverlening, zoals voorlichting, informatieverstrekking, hulp en ondersteuning en het '*empoweren*' van mensen door hen middelen aan te bieden waarmee zij bij organisaties hun rechten kunnen uitoefenen, handelen wij proactief. Het uitgangspunt hierbij is de eigen verantwoordelijkheid van mensen en organisaties. Organisaties worden gestimuleerd om op een goede en '*accountable*' manier met persoonsgegevens om te gaan.
De informatie uit het systeemtoezicht en de signalen, meldingen en klachten die wij ontvangen, worden geanalyseerd met als doel trends en risico's in kaart te brengen. Door het in kaart brengen van trends en risico's zorgen wij ervoor dat wij niet alleen reageren op actualiteiten, maar ook proactief onze eigen beleids- en onderzoekskeuzes maken.

3. De Autoriteit Persoonsgegevens neemt een actieve rol in de uitwerking van Europese regels en in de samenwerking met de andere Europese toezichthouders

Internationale samenwerking is niet alleen een ambitie, maar ook een vereiste die volgt uit de AVG. De AP vervult van oudsher een belangrijke rol in de samenwerking tussen de privacytoezichthouders en zal deze rol ook onder de nieuwe wetgeving voortzetten. Wij streven naar verhoging van de privacybescherming in de hele EU en behandelen klachten die afkomstig kunnen zijn van burgers uit alle EU-landen over

bedrijven die in Nederland gevestigd zijn of die in Nederland hun diensten aanbieden. Wanneer daarbij sprake is van een mogelijke inbreuk op de bescherming van persoonsgegevens van Nederlandse burgers door een bedrijf dat in een ander EU-land is gevestigd, zoeken wij nadrukkelijk de Europese samenwerking op. Hierbij gaat het onder meer om het gezamenlijk uitvoeren van onderzoeken en afstemmen van handhavingsmaatregelen. Daarnaast nemen wij actief deel aan internationale samenwerkingsverbanden van privacytoezichthouders. De kennis die wij hierbij opdoen, dragen wij actief uit naar organisaties en mensen in Nederland.

1.4 Kernwaarden

De AP handelt volgens vier kernwaarden: onafhankelijk, open, deskundig en effectief.

Onafhankelijk

De Autoriteit Persoonsgegevens is een onafhankelijke toezichthouder zonder invloed van bedrijven en overheden. We houden rekening met de belangen van anderen, maar behouden tegelijkertijd onze onafhankelijke positie. Altijd met een onbevooroordeelde en scherpe blik.

De AP houdt rekening met de belangen van alle betrokken partijen, maar tegelijkertijd bepalen en formuleren wij zelfstandig en weloverwogen onze standpunten en prioriteiten. De onafhankelijkheid komt ook tot uitdrukking in de manier waarop de oordeelsvorming in onderzoeken tot stand komt: wij doen feitelijk, met een scherpe blik en onbevooroordeeld onderzoek.

Open

De Autoriteit Persoonsgegevens staat in verbinding met haar omgeving. Mensen en organisaties weten ons te vinden met signalen en voor informatie over de regels en risico's. We zijn transparant waar het kan. We communiceren actief over ons werkproces en onze besluiten, stimuleren het publieke debat en geven duiding aan de regels. Toegankelijk taalgebruik en transparantie over ons handelen dragen bij aan onze effectiviteit en vergroten de legitimiteit ervan.

Openheid betekent dat de AP er uitdrukkelijk voor kiest om actief naar buiten te treden, contact te houden met het toezichtsveld en goed bereikbaar is voor alle mensen en organisaties. Daarbij houden we nadrukkelijk rekening met het gegeven dat niet alle burgers zich in dezelfde mate zelfstandig kunnen redden in hun contact met organisaties. Wij willen een gesprekspartner zijn wanneer het gaat om het implementeren van een hoog niveau van gegevensbescherming in organisaties. Wij denken graag mee over de wijze waarop bedrijven en overheden innovatieve producten en diensten privacyvriendelijk kunnen ontwikkelen. Daarnaast zijn wij transparant over onze verrichte werkzaamheden, doelen en middelen en leggen wij verantwoording af over onze resultaten. Wij communiceren enerzijds over geconstateerde overtredingen en hebben anderzijds nadrukkelijk aandacht voor het (proactief) communiceren van situaties waarin de bescherming van persoonsgegevens op een goede wijze is geborgd.

Deskundig

Medewerkers van de Autoriteit Persoonsgegevens zijn ter zake kundig en ontwikkelen voortdurend mee met hun omgeving. De AP stimuleert de ontwikkeling van individuele medewerkers en werkt aan de organisatie als geheel om een moderne toezichthouder te zijn.

De AP kent een belangrijke waarde toe aan haar deskundigheid. Onze deskundigheid krijgt vorm door ervoor te zorgen dat de medewerkers beschikken over de vereiste vakkennis, professioneel optreden en betrokkenheid tonen. Wij zien professionalisering als een voortdurende eis aan alle mensen binnen onze

organisatie. Wij investeren in de opleiding van onze medewerkers. Daarbij zoekt de AP ook de samenwerking met andere toezichthouders, openbaar bestuur en universiteiten. Deskundigheid betekent ook dat onze medewerkers weten wat er speelt. Op basis van gedegen kennis over een thema of toezichtsgebied, bepaalt de AP proactief haar positie en kiest zij voor een inzet van instrumenten die het meest effectief is binnen dat thema of toezichtsgebied.

Effectief

Omdat we moeten reageren op nationale én internationale ontwikkelingen maken we weldoordachte keuzes. Per situatie kiezen we voor de meest effectieve aanpak. Met daadkracht, maar altijd met focus op het grondrecht van mensen.

Het toezichtsveld van de AP is groot en met het van toepassing worden van de AVG krijgt de AP er een aantal aanzienlijke taken bij. Dit betekent dat wij prioriteiten moeten stellen, slim moeten omgaan met het uitvoeren van interventies en de capaciteit zo effectief en efficiënt mogelijk moeten inzetten. Om dit te kunnen realiseren zoeken we de samenwerking op met diverse brancheorganisaties en andere stakeholders. Meer in het bijzonder richten wij ons op de Functionarissen Gegevensbescherming (FG's). FG's zijn te beschouwen als de interne toezichthouders van organisaties: zij houden intern toezicht op de toepassing en naleving van de AVG.

Effectief toezicht vereist daadkracht. Om een effectieve toezichthouder te kunnen zijn past de AP uiteenlopende toezichts- en handhavingsinstrumenten toe. Daarbij kan onder meer worden gedacht aan het versturen van een waarschuwingsbrief, het aangaan van een normoverdragend gesprek, het starten van een onderzoek, het opleggen van een dwangsom of het opleggen van een boete. Als uitgangspunt geldt dat wij kiezen voor het handhavingsinstrument dat het minst ingrijpend is en waarmee het meeste effect wordt bereikt. Overigens wordt daadkracht niet alleen bepaald door een goed lopend interventiebeleid. Ook deskundig informeren, adviseren en communiceren kenmerken een daadkrachtige houding. Dit betekent dat wij daar waar mogelijk *'guidance'* bieden, maar ook zullen optreden wanneer dit nodig is.

2. Toezicht 2018-2019

2.1 Bevorderen van de naleving

Het belangrijkste doel van ons toezicht is het bevorderen van de naleving van de privacywetgeving. Voorafgaand aan de inwerkintreding van de AVG heeft de AP dan ook veel aandacht besteed aan bewustwording van mensen, bedrijven en overheden over de veranderingen die de nieuwe wetgeving met zich meebrengt. Wij hebben campagne gevoerd, presentaties gegeven en workshops verzorgd. De telefonische bereikbaarheid is vergroot en er zijn praktische hulpmiddelen ter beschikking gesteld waarmee bedrijven en organisaties hun bedrijfsvoering AVG-proof kunnen maken.

Bieden van '*guidance*'

Ook het komende jaar richt de AP zich op de bevordering van de naleving van de privacywetgeving, onder meer door het bieden van *´guidance´*. Dit doen wij door het geven van voorlichting en advies aan mensen en organisaties. Ook ondersteunen wij organisaties door het aanbieden van praktische hulpmiddelen, geven wij een duidelijke normuitleg en bevorderen wij de totstandkoming van Europees gedragen normen. Verder beoordelen wij verzoeken tot voorafgaande raadplegingen en vergunningaanvragen voor het verwerken van strafrechtelijke gegevens en bevorderen wij de totstandkoming van onder meer gedragscodes. Wij investeren tevens in het opzetten en onderhouden van een goede relatie met FG's. Wij zorgen ervoor dat wij goed bereikbaar zijn voor FG's, geven voorlichting en beantwoorden eventuele vragen die zij hebben.

Behandeling van klachten

Onder de AVG is het klachtrecht versterkt. De AP neemt klachten in behandeling die wijzen op een mogelijke inbreuk op de verwerking van persoonsgegevens van mensen. Het Informatie- en Meldpunt Privacy is vijf dagen per week telefonisch bereikbaar om vragen, signalen en klachten in behandeling te nemen. De AP beoogt met het behandelen van klachten mensen te versterken in het uitoefenen van hun recht. Om mensen te helpen bij het uitoefenen van hun recht bieden wij hulpmiddelen aan en ondersteunen en begeleiden wij hen waar nodig. Zo nodig zullen wij naar aanleiding van een klacht actief optreden bij een overtreding. Het behandelen van klachten draagt daarmee bij aan de bevordering van de naleving van de wet.

Wetgevingsadvies

In haar rol als wetgevingsadviseur bevordert de AP dat wet- en regelgeving in lijn is met het Handvest van de Grondrechten van de EU, het Verdrag betreffende de Werking van de Europese Unie (VWEU) en de AVG. Wij beoordelen onder meer of de inbreuk op het recht op bescherming van persoonsgegevens gerechtvaardigd is en niet bovenmatig is gelet op het doel dat met de regelgeving wordt nagestreefd. De AP betrekt daarbij de kennis en ervaring die zij opdoet in contact met het toezichtsveld en bij het uitoefenen van haar toezichts- en handhavingsbevoegdheden.
De AP geeft zowel gevraagd als ongevraagd advies aan en treedt in overleg met de wetgever. Wij denken actief mee over actuele vraagstukken over het gebruik van persoonsgegevens met als doel een behoorlijke en rechtmatige dienstverlening door de overheid te bevorderen.

2.2 Controleren van de naleving

Naast het bieden van *'guidance'* en het behandelen van klachten om de naleving te bevorderen, is het ook belangrijk om de (mate van) naleving te controleren. Bedrijven en overheden moeten aantonen dat zij in overeenstemming handelen met de AVG.

De verantwoordingsplichten in de AVG dwingen organisaties aan te tonen dat zij voldoen aan de AVG. Het op orde hebben van de verantwoordingsplichten wil niet per definitie zeggen dat een organisatie volledig voldoet aan de AVG. Het is echter wel een goede indicatie van de mate waarin serieus werk is gemaakt van de implementatie van de AVG en dat is nagedacht over belangrijke onderdelen uit de AVG (zoals grondslagen, doelbinding en beveiliging).

Om vast te stellen of aan de verantwoordingsplichten van de AVG is voldaan, wordt in verschillende sectoren de naleving van één van deze plichten uit de AVG gecontroleerd. Daarbij is de verwachting dat informatie over de uitkomsten van de controles het lerend vermogen van organisaties ten aanzien van de naleving van de AVG zal vergroten. Wij zullen dan ook actief communiceren over de controles en onze bevindingen.

2.3 Risicogericht toezicht

In lijn met de AVG stelt de AP de burger centraal. Gegevensverwerkingen zijn voor burgers in toenemende mate onzichtbaar. De AP hanteert in haar toezicht een risicogerichte aanpak waarbij zij extra oog heeft voor mogelijke inbreuken op de bescherming van persoonsgegevens waarbij grote groepen mensen kunnen worden geraakt. Daarbij richt zij zich de komende periode in het bijzonder op de overheid, de zorg en bedrijven die handelen in persoonsgegevens. De AP zal ook optreden bij andere sectoren, bijvoorbeeld naar aanleiding van de actualiteit en naar aanleiding van klachten.

De overheid

Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid, vaak gevoelige, persoonsgegevens. Burgers zijn veelal verplicht om hun persoonsgegevens af te geven. Zij moeten er dan ook op kunnen vertrouwen dat de overheid zich bij de verwerking van de persoonsgegevens aan de regels houdt.

De AP legt extra focus op zowel de beveiliging van persoonsgegevens als de vraag of de verwerking van de persoonsgegevens gebaseerd is op de juiste grondslag. Vooral daar waar uitwisseling van deze gegevens aan de orde is. Verder voeren wij controles uit op de naleving van de verplichting om een register van verwerkingen op te stellen, de verplichting om een FG aan te stellen, alsmede de wijze waarop de organisatie de FG positioneert en hem in staat stelt de taken en verplichtingen te vervullen die hij op grond van de AVG heeft.

De zorg

Naast overheden beschikken ook zorginstellingen over grote hoeveelheden persoonsgegevens. Daarbij gaat het vaak om medische gegevens. Gegevens over iemands gezondheid zijn wegens hun gevoelige aard bijzondere persoonsgegevens. De AVG stelt, net als de voormalige Wet bescherming persoonsgegevens (Wbp), aan de verwerking van deze bijzondere persoonsgegevens dan ook strengere eisen. Een goede beveiliging is belangrijk om te voorkomen dat de medische gegevens van patiënten in handen komen van

onbevoegden. Patiënten moeten er overeenkomstig het medisch beroeps geheim vanuit kunnen gaan dat hun medische gegevens een zaak is tussen hen en de behandelend(e) arts(en).

De AP legt ook bij zorginstellingen extra focus op de beveiliging van medische gegevens en op de vraag of de verwerking gebaseerd is op de juiste grondslag. Vooral daar waar uitwisseling van deze gegevens aan de orde is. Ook hier zal de AP toezien op de naleving van de verplichting om een register van verwerkingen op te stellen, de verplichting om een FG aan te stellen, alsmede de wijze waarop de organisatie de FG positioneert en hem in staat stelt de taken en verplichtingen te vervullen die hij op grond van de AVG heeft.

De handel in persoonsgegevens

De handel in persoonsgegevens is de afgelopen jaren toegenomen. Datahandelaren verzamelen op grote schaal persoonsgegevens van consumenten via een groot aantal verschillende online en offline bronnen. Zij verwerken deze tot profielen en verstrekken of verkopen deze gegevens vervolgens aan andere datahandelaren en/of afnemers die besluiten nemen over bijvoorbeeld de kredietwaardigheid van mensen of de gegevens gebruiken voor direct marketing-doeleinden. De meest bekende datahandelaren zijn de zogeheten handelsinformatiebureaus, maar er zijn veel meer bedrijven en organisaties die persoonsgegevens verhandelen waarover zij – veelal ten behoeve van een ander doel- beschikken. Mensen weten vaak niet om hoeveel gegevens het gaat, welke persoonsgegevens worden verstrekt aan welke partijen en met welk doel. Ook zijn mensen doorgaans niet op de hoogte van profilering. Er is een groot risico voor burgers als zij niet op de hoogte zijn van verwerkingen van hun gegevens en de daarop volgende verstrekking van hen betreffende profielen aan andere partijen. Zij komen er mogelijk pas achter nadat een beslissing is genomen die hen raakt, zoals het weigeren van een lening of abonnement. Een ander risico is dat sommige gegevens of opgestelde profielen onjuist zijn, met mogelijk verstrekkende gevolgen voor mensen. Mensen verliezen op deze wijze zeggenschap over hun gegevens.

De AP richt zich de komende periode op de handel in persoonsgegevens met als primair doel te bevorderen dat bedrijven en organisaties die persoonsgegevens verkopen dit alleen doen op basis van een juiste grondslag en voldoen aan de informatieplicht onder de AVG.

Datalekken

Daar waar veel (gevoelige) persoonsgegevens worden verwerkt, nemen de risico's op en gevolgen van datalekken toe. Adequate beveiliging is dan ook van groot belang. Sinds het van kracht zijn van de meldplicht datalekken per 1 januari 2016 heeft de AP zich vooral gericht op het stimuleren van verantwoordelijken om datalekken te melden. Ontving de AP in 2016 bijna 6000 meldingen van datalekken, in 2017 waren dat er ruim 10.000. Een stijging van ruim 70%. In een aantal gevallen bleek de beveiliging niet of onvoldoende op orde. Dit brengt grote risico's met zich mee voor de bescherming van persoonsgegevens, met name wanneer als gevolg van onvoldoende beveiliging sprake is van een lek van bijzondere persoonsgegevens zoals medische gegevens en gegevens over politieke of seksuele voorkeur. . Maar ook als het gaat om de naam-, adres- en woonplaatsgegevens, creditcardgegevens, e-mailadressen, of zelfs het burgerservicenummer (BSN) van mensen.

De AVG stelt een aantal nieuwe eisen aan de meldplicht datalekken. Organisaties moeten bijvoorbeeld alle datalekken documenteren en niet alleen de gemelde datalekken. Zij moeten een register van datalekken bijhouden. Daarnaast zijn de boetes die kunnen worden opgelegd vanaf het van toepassing worden van de AVG hoger dan voorheen.

De AP geeft in 2018 -2019 extra aandacht aan niet-gemelde datalekken en datalekken die (mede) zijn veroorzaakt door ernstige tekortkomingen in de beveiliging.