



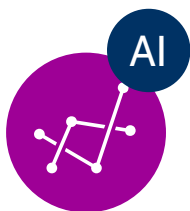
Beschermen van burgers in een digitale wereld

Leven in een vrije en veilige samenleving is een groot goed. Dat kan alleen wanneer wij onze grondrechten goed beschermen. Zonder de bescherming van ons grondrecht op gegevensbescherming kunnen andere grondrechten in gevaar komen. Zoals het recht op privacy en het recht om niet gediscrimineerd te worden. Als AP maken wij ons elke dag sterk voor een samenleving waarin persoonsgegevens goed beschermd worden. En het gebruik van algoritmes en artificiële intelligentie (AI) verantwoord gebeurt.



Toezicht houden betekent ook keuzes maken. Het toezichtveld van de AP wordt namelijk steeds groter en onze middelen zijn beperkt. Daarom richten we ons op de grootste risico's voor burgers en samenleving. De bescherming van publieke belangen staat altijd voorop. Zoals gelijke behandeling, persoonlijke autonomie en de controleerbaarheid van macht.

In 2024 zetten we een aantal specifieke thema's centraal. Dit doen we binnen en naast ons reguliere werk, zoals voorlichting geven, onderzoek doen, sancties opleggen, wetgeving toetsen en klachten en datalekken behandelen. In 2024 besteden we extra aandacht aan onderstaande vijf thema's:



Algoritmes & AI



Big Tech



Vrijheid & veiligheid



Datahandel



Digitale overheid



Algoritmes & AI

Algoritmes en AI zijn niet meer weg te denken uit onze samenleving. Algoritmes bieden een hoop kansen. Bijvoorbeeld voor het bedrijfsleven, de wetenschap en de medische wereld. Tegelijkertijd kan door onverantwoorde ontwikkeling of inzet van algoritmes grote schade ontstaan. Onjuiste data of data die gebaseerd zijn op foutieve aannames, kunnen zowel bij de overheid als bij bedrijven grote risico's voor burgers met zich meebrengen. Zoals uitsluiting of discriminatie. Dat willen we voorkomen door de risico's in kaart te brengen en handvatten te bieden voor veilig en verantwoord gebruik van algoritmes en AI.

Wat doen we in ieder geval in 2024?

- We geven prioriteit aan klachten, datalekken en onderzoeken die over algoritmes en AI gaan, zodat we zicht krijgen op waar en waarom dingen misgaan.
- We signaleren en analyseren overkoepelende risico's van algoritmes die in meerdere sectoren spelen. Twee keer per jaar publiceren we de Rapportage Algoritmerisico's Nederland (RAN).
- We geven uitleg over de risico's van algoritmes en communiceren 'best practices' over hoe algoritmes verantwoord zijn in te zetten.
- We werken samen met andere toezichthouders om ervoor te zorgen dat het toezicht op algoritmes goed is afgestemd.

Big Tech

De invloed van grote techbedrijven blijft groeien. Een klein aantal bedrijven heeft hierdoor veel macht. Omdat deze bedrijven ook veel persoonlijke gegevens in handen hebben, kunnen ze mensen beïnvloeden. Bijvoorbeeld door nepnieuws en politieke targeting op basis van profielen. Dat vormt een bedreiging voor onze democratie en samenleving. Om ervoor te zorgen dat grote techbedrijven zich aan de AVG houden, werkt de AP veel samen met andere Europese toezichthouders. En treden we hard op als dat nodig is.

Wat doen we in ieder geval in 2024?

- We doen (internationaal) onderzoek naar overtredingen door grote techbedrijven. Klachten over deze bedrijven behandelen we met voorrang. Voor het onderzoek kunnen we speciale instrumenten inzetten.
- Samen met de andere Europese toezichthouders dragen we eraan bij dat grote techbedrijven alleen generatieve AI-modellen ontwikkelen en aanbieden die voldoen aan de wet en veilig zijn voor mensen, nu en in de toekomst.
- We werken samen met onze Europese collega's aan innovatieve manieren om het toezicht op big tech effectiever vorm te geven, om zo de grondrechten van burgers nog beter te beschermen.

Vrijheid & veiligheid

Vrijheid en veiligheid kunnen op gespannen voet met elkaar staan. Om de veiligheid te vergroten, moeten er soms maatregelen worden genomen die de vrijheid beperken. Omdat vrijheid en veiligheid voor mensen beide van fundamenteel belang zijn, moet een zorgvuldige afweging worden gemaakt tussen meer van het een en minder van het ander. Als AP letten we bij de verwerking van persoonsgegevens extra op een verdedigbare balans tussen vrijheid en veiligheid.

Wat doen we in ieder geval in 2024?

- We doen onderzoek naar en houden toezicht op grote Europese informatiesystemen en databases die worden gebruikt voor het beschermen van de buitengrenzen van het Schengengebied.
- Bij de inzet van nieuwe, risicovolle technologieën in het veiligheidsdomein adviseren we gevraagd en ongevraagd over wat wel en niet mag, om zo te voorkomen dat grondrechten in het geding komen.
- Het gebruik van gezichtsherkenningstechnologie om de veiligheid te vergroten brengt ook grote risico's voor burgers met zich mee. De AP besteedt hier extra aandacht aan en geeft praktische handvatten voor veilig gebruik.

Datahandel

De steeds meer gedigitaliseerde ('slimme') producten en diensten die we gebruiken, creëren veel waardevolle data. Met als gevolg dat er ook steeds meer ongeoorloofde (door)verkoop plaatsvindt van persoonsgegevens. Niet alleen in Nederland, maar ook internationaal. Dat moeten we een halt toeroepen.

Wat doen we in ieder geval in 2024?

- We starten een meerjarenproject dat het ongeoorloofd online volgen van mensen, bijvoorbeeld met cookies, op verschillende fronten aanpakt.
- We geven prioriteit aan onderzoek naar klachten en datalek-meldingen die een duidelijke link hebben met datahandel.
- We zetten extra in op voorlichting en communicatie over naleving op het gebied van datahandel. Zo zorgen we ervoor dat bedrijven zich aan de wet houden en burgers geen schade oplopen.

Digitale overheid

De overheid beschikt over veel – vaak gevoelige – persoonsgegevens van Nederlandse burgers en maakt hier veel gebruik van. Het risico dat burgers in de knel komen is groot als de overheid verkeerd omgaat met hun persoonsgegevens. Bovendien heeft de overheid een voorbeeldfunctie als het gaat om de verantwoorde omgang met persoonsgegevens. Om ervoor te zorgen dat overheidsorganisaties veilig omgaan met persoonsgegevens schenken we hier extra aandacht aan en delen we onze kennis hierover.

Wat doen we in ieder geval in 2024?

- We reserveren extra capaciteit om onderzoek te doen naar overheden en uitvoeringsorganisaties die persoonsgegevens van burgers gebruiken in algoritmes.
- We besteden opnieuw aandacht aan het delen van gegevens tussen verschillende onderdelen van de overheid en andere organisaties. Daarnaast geven we aandacht aan de risico's van het gebruik van algoritmes bij de overheid, zoals discriminatie.
- We delen gevraagd en ongevraagd kennis over gegevensuitwisseling in het sociaal domein en over privacywaarborgen bij fraudebeleid en schuldhulpverlening.

Wat kunnen we (nog steeds) niet doen?

- Alle klachten op tijd afhandelen. Mensen moeten nog altijd te lang wachten op de afhandeling van hun klacht. Het duurt vaak meer dan een half jaar voordat we een klacht kunnen oppakken. Ook onderzoek doen, al dan niet naar aanleiding van een klacht, komt door capaciteitsgebrek in het geding.
- Alle datalekken de aandacht geven die ze verdienen. Met alle gevolgen van dien voor de slachtoffers van deze datalekken.
- Bedrijven en internationale organisaties helpen om een vergunning

te krijgen voor de veilige doorgifte van persoonsgegevens naar landen buiten de Europese Economische Ruimte (EER). Voor een BCR-vergunning is de wachttijd nu gemiddeld 6 jaar.

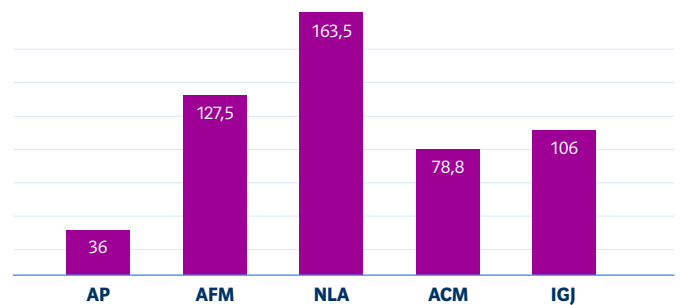
- Proactief advies geven over wetgeving, zodat persoonsgegevens goed zijn beschermd in de wet.
- Sectoren die veel persoonsgegevens verwerken de aandacht geven die nodig is. Bijvoorbeeld de zorg, het onderwijs, de energiesector, de overheid en de financiële sector.

Extra budget voor de AP: een doorkijkje naar de toekomst

In het regeerakkoord uit 2021 is een jaarlijkse verhoging van het budget van de AP vastgelegd. Tot en met 2026 groeit ons budget ieder jaar licht. Dat is mooi, maar het is nog niet genoeg. De financiering van het toezicht van de AP blijft ver achter op de hoge mate van digitalisering van Nederland. Al helemaal met de snelle opkomst van AI, want algoritmes en AI verwerken vaak persoonsgegevens. Hetzelfde geldt voor cybersecurity. Online veiligheid en de bescherming van persoonsgegevens gaan hand in hand, maar die link wordt nog maar weinig gelegd. Terwijl cybersecurity, informatiebeveiliging en privacy noodzakelijk zijn voor digitale veiligheid. Om onze taak goed te kunnen vervullen, moet ons structurele budget groeien naar tenminste 100 miljoen euro per jaar.

AP Budget per jaar	2024	2025	2026	2027
Totaal in miljoenen €	40	43	44	44

AP in vergelijking met andere toezichthouders



CIJFERS UIT 2023. BEDRAGEN IN MILJOENEN EURO.

AP = Autoriteit Persoonsgegevens, AFM = Autoriteit Financiële Markten, NLA = Nederlandse arbeidsinspectie, ACM = Autoriteit Consument & Markt, IGJ = Inspectie Gezondheidszorg en Jeugd

Samen onze aandachtspunten bepalen

De invloed van technologie op onze samenleving en democratische rechtsstaat is enorm. Dat raakt ook het toezicht van de AP. We vinden het daarom heel belangrijk om samen op te trekken met (vertegenwoordigers van) burgers, bedrijven, de wetenschap en de politiek om onze aandachtspunten voor de komende jaren te bepalen. In 2024 gaan we nog intensiever met deze externe stakeholders in overleg over de toezichtagenda van de AP.

