13 mei 2026

Digitale weerbaarheid begint bij een solide basis

Gegevensbescherming en digitale veiligheid zijn onlosmakelijk met elkaar verbonden. Wanneer er persoonsgegevens bij ingrijpende cyberincidenten betrokken zijn, zijn de risico's voor mensen, bedrijven en (overheids)organisaties groot. Mensen riskeren dat hun vertrouwen, om bijvoorbeeld gegevens met zorginstellingen of overheden te delen, verloren gaat. Onze digitale economie kan daaronder lijden en mensen lopen risico op openbaarmaking van soms zeer gevoelige gegevens en op misbruik van gegevens, zoals identiteitsfraude. De Autoriteit Persoonsgegevens (AP), de onafhankelijke toezichthouder die mensen beschermt in een digitale wereld, ziet dat er door de gehele samenleving heen nog veel winst te boeken valt als het aankomt op cyberveiligheid.

De AP constateert 3 broodnodige verbeteringen voor de cyberveiligheid van Nederland:

Voor bedrijven, (overheids)organisaties en ICT-leveranciers

1. **Zorg voor een hoog beveiligingsniveau.** Het algemene beveiligingsniveau van bedrijven, organisaties en ICT-leveranciers blijft al jaren te laag. Deze organisaties moeten zelf in actie komen. Dat begint bij het in kaart brengen van risico's. En daar de beveiligingsmaatregelen op afstemmen.
2. **Beperk de gevolgen van een datalek** door in te zetten op dataminimalisatie, naleving van bewaartermijnen en adequate informatievoorziening voor slachtoffers na een datalek.

Voor het kabinet en de politiek

3. **Garandeer adequaat toezicht** om Nederland digitaal weerbaar te maken en te houden en maak het mogelijk dat de AP meer risico-gestuurd preventief toezicht kan houden.

Risico-gestuurd toezicht op de beveiliging van persoonsgegevens

Cyberincidenten en datalekken zijn aan de orde van de dag. Ook in het toezicht ziet de AP dit terug. Onderdeel van dat toezicht is namelijk een meldplicht voor datalekken. In 2025 werden er ruim 44.000 datalekken bij de AP gemeld.[1] In 2024 waren dat er nog ongeveer 38.000.[2]

Door de grote hoeveelheid meldingen moet de AP keuzes maken. Daarom houdt de AP risico-gestuurd toezicht. We richten ons zoveel mogelijk op datalekken die de grootste risico's opleveren voor slachtoffers. De AP doet dit aan de hand van het wettelijke kader uit de Algemene verordening gegevensbescherming (AVG). De AP beoordeelt of organisaties ten tijde van het incident de beveiliging op orde hadden en of zij naar behoren hebben voldaan aan de meldplicht (zowel aan slachtoffers als aan de AP). Ook controleert de AP of organisaties hebben gehandeld volgens de privacybeginselen.[3] Daarnaast houdt de AP ook doorlopend toezicht op patronen en trends in cyberincidenten. Aan het houden van toezicht op het beveiligingsniveau zonder dat er sprake is van een lek (preventief toezicht) komt de AP helaas nauwelijks toe.

De AP houdt op 3 manieren toezicht op datalekken:

a. **Direct ingrijpen bij impactvolle hacks**. Bijvoorbeeld door erop toe te zien dat organisaties slachtoffers snel en goed informeren bij een datalek.[4] Zo wordt de weerbaarheid van slachtoffers vergroot.

[1] De AP geeft jaarlijks meer inzicht in de ontwikkelingen, zorgen en gevaren op het gebied van datalekken en cyberaanvallen in de Datalekkenrapportage. De nieuwste rapportage over het jaar 2025 wordt voor de zomer gepubliceerd.
[2] Cijfers uit Datalekkenrapportage AP 2024.
[3] Zie de bijlage van dit position paper voor een uitwerking van het wettelijk kader bij toezicht op datalekken, inclusief onze definitie van een datalek en uitleg over onze rol bij de Cyberbeveiligingswet (Cbw), die naar verwachting medio 2026 in werking treedt.
[4] Zoals bij de casus AddComm, zie: Datalekkenrapportage AP 2024, p. 15-17.

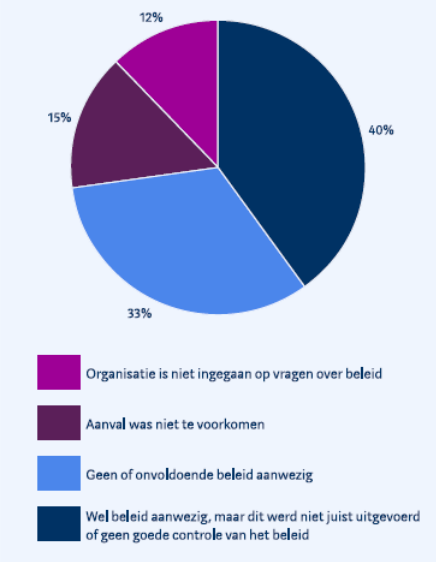
b. **Doorlopend toezicht op patronen en trends.** De AP heeft door de datalekmeldingen een uniek beeld van wat er goed en fout gaat bij organisaties. De AP gebruikt die kennis om patronen en nieuwe trends te herkennen. Daar speelt de AP op in, bijvoorbeeld met verkennende onderzoeken en aanbevelingen voor bepaalde sectoren.
c. **Formeel onderzoek bij ernstige overtredingen**. Als de AP ernstige overtredingen vaststelt, kan de AP een formeel onderzoek starten en een boetetraject in gang zetten. De preventieve, afschrikwekkende werking van het opleggen van boetes is een belangrijk onderdeel van het werk van de AP als toezichthouder. De keerzijde is dat formeel onderzoek bijzonder veel capaciteit vraagt. Die capaciteit heeft de AP op dit moment onvoldoende, in verhouding tot het aantal grote cyberincidenten.

Een solide basis als fundament van een weerbare digitale wereld

De AP heeft een unieke positie. De AP beschikt door de meldplicht voor datalekken over veel informatie over de cyberveiligheid van bedrijven, (overheids)organisaties en ICT-leveranciers. Deze informatie geeft inzicht in waar verbeteringen broodnodig zijn.

Zorg voor een hoog beveiligingsniveau

De AP constateert al meerdere jaren op rij dat het beveiligingsniveau van bedrijven en organisaties over het algemeen zowel technisch als organisatorisch te laag ligt. Organisaties geven desgevraagd in een rapportage zelf aan dat zij denken dat de incidenten veroorzaakt worden door gebrek aan beleid. Dat geldt voor 33% van de onderzochte organisaties. Nog vaker is er wel beleid, maar voeren organisaties het niet juist uit of controleren zij de uitvoering onvoldoende. Dat geldt voor 40% van de onderzochte organisaties.[5] Dit maakt organisaties zeer kwetsbaar. Zij moeten zelf in beweging komen om die kwetsbaarheid weg te nemen en digitaal weerbaar te worden. Dat begint bij het op orde krijgen van de basis en het in kaart brengen van risico's.



De AP drukt organisaties op het hart om goed inzicht te krijgen in risico's en te nemen maatregelen, en om kritisch na te denken over het verwerken en bewaren van gegevens. Ook moeten zij verantwoordelijkheid en controle pakken door cyberveiligheid niet op het bord van individuele medewerkers te schuiven, maar centraal te borgen en hoog op de agenda van bestuurders te plaatsen. Audits, beveiligingstests en technische waarborgen zijn hierbij essentieel om fouten vroegtijdig te detecteren en verhelpen.

Bedrijven en organisaties nemen veelvuldig diensten en producten af van ICT-leveranciers. Hierdoor geldt dat als ICT-leveranciers hun digitale veiligheid op orde hebben dit de gehele keten veiliger en weerbaarder maakt. Recent kondigde de AP aan om ICT-leveranciers preventief te gaan controleren op hun digitale beveiliging. Zo wil de AP datalekken veroorzaakt door een laag beveiligingsniveau helpen voorkomen en een veilig digitaal ondernemersklimaat stimuleren.

Tref maatregelen die de gevolgen van een datalek verkleinen

Een datalek kan iedere organisatie overkomen. Het is daarom niet alleen belangrijk om beveiligingsmaatregelen te treffen om datalekken te *voorkomen,* organisaties dienen ook maatregelen te treffen die de gevolgen van een datalek *verkleinen*. Te denken valt aan:

1. dataminimalisatie als uitgangspunt nemen (alleen de strikt noodzakelijke gegevens verwerken);

[5] Cijfers uit Datalekkenrapportage AP 2024 op basis van zelf-rapportage.

2. bewaartermijnen naleven (die gegevens tevens niet langer bewaren dan strikt noodzakelijk is);
3. het garanderen van adequate informatievoorziening voor slachtoffers na een datalek (door het snel verstrekken van duidelijke waarschuwingsberichten).

Momenteel ziet de AP nog te vaak dat organisaties niet voldoen aan deze basismaatregelen.

Garandeer adequaat toezicht

Om ervoor te zorgen dat Nederland digitaal weerbaar is en blijft, is adequaat toezicht op het beveiligingsniveau via zowel de AVG als de Cyberbeveiligingswet (Cbw) essentieel.[6] De AP heeft het breedste beeld als het gaat om datalekken. Dit maakt dat de AP hier een centrale rol speelt. Incidenten kunnen door adequaat en efficiënt toezicht, en op basis van samenwerking tussen toezichthouders en ketenpartners, beter worden behandeld en mogelijk zelfs voorkomen worden.

In een tijd waar datalekken aan de orde van de dag zijn, zou de AP fors meer tijd moeten kunnen spenderen aan preventief toezicht op bijvoorbeeld het naleven van de verplichting om adequate technische en organisatorische maatregelen te treffen op dataminimalisatie en bewaartermijnen. Daar heeft de AP echter nauwelijks capaciteit voor.

Daarnaast is het belangrijk dat het voor de markt en brede samenleving duidelijk is dat gebrekkige beveiliging van gegevens gevolgen kan hebben. Als organisaties bijvoorbeeld worden gehackt omdat de beveiliging niet op orde was, kan er een sanctie volgen. Zo komen organisaties in beweging om zelf hun cyberveiligheid op orde te brengen. Voorkomen blijft echter wel beter dan genezen.

De AP zou daarom het risico-gestuurd preventief toezicht sterk moeten kunnen intensiveren en vaker onderzoeken moeten starten die tot een sanctie kunnen leiden. Maar hiervoor heeft de AP nu beperkte capaciteit. In een wereld waar datalekken, cyberaanvallen en het aantal slachtoffers alleen maar lijken toe te nemen, kan de AP niet anders dan hier aandacht voor vragen.

Tot slot

De solide basis die in dit paper is geschetst, ziet de AP als een voorwaarde voor het cyberveilig en weerbaar maken en houden van Nederland. Deze basis garanderen is essentieel voor het vertrouwen van mensen in de digitale wereld en het ontwikkelen van onze digitale economie.

Het is de kern van het werk van de AP om dit vertrouwen in stand te houden, mensen grip te geven op hun gegevens en om tegelijkertijd bedrijven en (overheids)organisaties te ondersteunen in het veilig houden van die gegevens.

Vanzelfsprekend is de AP altijd bereid om hierover met u als leden van de Tweede Kamer nader in gesprek te gaan.

[6] Uit recent onderzoek van EenVandaag blijkt dat zo'n 74% van de bevraagde mensen vindt dat bedrijven waar persoonsgegevens lekken harder gestraft moeten worden.

Bijlage

Definitie van een datalek

Een datalek houdt in dat er sprake is van een beveiligingsinbreuk die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens. Daar is bijvoorbeeld sprake van als een cybercrimineel gegevens versleutelt, waardoor de organisatie er niet meer bij kan. Of als een cybercrimineel gegevens steelt.

Wettelijk kader bij toezicht bij datalekken

Artikel 5 AVG bevat de beginselen en is daarmee het fundament van de AVG. In het licht van datalekken zijn met name de beginselen dataminimalisatie, opslagbeperking en beveiliging belangrijk. Persoonsgegevens moeten:

- toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (dataminimalisatie);
- worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (opslagbeperking);
- 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 (beveiliging).

Belangrijke specifieke regels voor het voorkomen en afhandelen van datalekken staan in de artikelen 32, 33 en 34 van de AVG.

Artikel 32 AVG luidt dat "*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 (...).*"

- Dit vergt van organisaties dat een risico-inventarisatie wordt gemaakt om vast te stellen wat een op het risico afgestemd beveiligingsniveau is. Organisaties en hun leveranciers moeten beveiligingsmaatregelen nemen om dit beveiligingsniveau te waarborgen. In de term waarborgen ligt besloten dat beveiliging een continu proces is en geen momentopname. De organisaties zullen regelmatig moeten controleren of de beveiligingsmaatregelen die ze hebben genomen voldoende zijn ten opzichte van de risico's en toenemende (cyber)dreigingen.
- Organisaties moeten datalekken met beveiligingsmaatregelen waar mogelijk voorkomen en wanneer er toch een datalek plaatsvindt er tijdig op kunnen reageren. Dat houdt in dat organisaties datalekken snel moeten kunnen opsporen (logging en monitoring) en daar adequaat actie op kunnen nemen.

Artikel 33 AVG bepaalt dat datalekken binnen 72 uur bij de AP moeten worden gemeld, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor natuurlijke personen. Doel van deze bepaling is dat de AP wordt geïnformeerd over een datalek en snel kan ingrijpen indien:

- betrokkenen niet (goed) worden geïnformeerd,
- de organisatie niet voldoende maatregelen neemt om het datalek te beëindigen of om nieuwe datalekken te voorkomen.

Artikel 34 bepaalt dat organisaties mensen snel moeten informeren over datalekken die een hoog risico inhouden. Doel van deze bepaling is dat slachtoffers informatie ontvangen over de risico's van het datalek en over de maatregelen die zij kunnen nemen om zich tegen de mogelijke gevolgen ervan te beschermen.

Naast de AVG, houdt de AP ook toezicht op de naleving van de Richtlijn gegevensbescherming bij rechtshandhaving (RGR), die vergelijkbare regels als de AVG bevat maar dan gericht op politie en justitiële gegevens.

De Cyberbeveiligingswet en de AP

De AP is geen toezichthouder op de Cyberbeveiligingswet (Cbw), maar speelt er wel een belangrijke rol in. Alle organisaties die onder de Cbw vallen, verwerken persoonsgegevens en vallen daarmee ook onder het toezicht van de AP. Bij grote datalekken betekent dit dat zowel de Cbw-toezichthouder als de AP bevoegd is om op te treden richting deze organisaties. Als er bij een incident iets mis was in de beveiliging wat zowel onder de AVG (beveiliging van persoonsgegevens) als de Cbw (beveiliging van de dienst) valt, dan is het zo dat de AP voorrang heeft op het opleggen van een boete. Goede samenwerking tussen de AP en andere toezichthouders is essentieel.

Voor adequaat toezicht is tevens adequate implementatie van wetgeving een vereiste. De AP drukt het kabinet en de Kamer daarom op het hart snel werk te maken van de implementatie van de Cbw.