**Het lijkt het erop dat er vrijheid is voor bedrijven om te kiezen wie van hun klanten zij wel of niet informeren na een datalek, op basis van hun eigen afweging. Waarom moeten niet alle mensen van wie persoonsgegevens bewaard worden geïnformeerd worden na een datalek?**

·         Organisaties hebben zeker niet de vrijheid/ keuze om betrokkenen wel of niet te informeren.

·         Als er sprake is van een hoog risico voor de rechten en vrijheden van betrokkenen (zo staat het in de wet) dan moet de organisatie ze informeren. Dat is een verplichting. De AVG geeft aan wanneer er sprake is van hoog risico en wanneer niet. Zie ook onze website. De AP ziet daarop toe. En wij dragen organisaties op getroffen mensen te informeren, waar dat nodig is. Lees ook onze informatie [over meldplicht datalekken](https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken) en de [Richtsnoeren voor de melding van datalekken](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf).

**Onze deskundige in de uitzending vindt dat de AP strenger zou moeten controleren dat bedrijven gegevens ook op tijd *verwijderen*, zodat datalekken minder groot kunnen zijn. In hoeverre wordt nu door de AP gecontroleerd of bedrijven persoonsgegevens wel tijdig verwijderen?**

·         Als organisaties of bedrijven langer bewaren, en we krijgen daar signalen over, dan eisen wij informatie op of doen er onderzoek naar. Het is de eigen verantwoordelijkheid van organisaties om gegevens op tijd te verwijderen.

·         Het informeren van getroffen mensen is topprioriteit en is het eerste waar de AP naar kijkt. Of dat op tijd is gebeurd, en op de juiste manier.

·         We zitten op dit moment helaas met een groot tekort aan menskracht en budget, waardoor allerlei zaken vertraging oplopen. Dat heeft gevolgen voor het uitvoeren van de wettelijke taken van de AP.

**Een consument die in de uitzending aan bod komt kwam erachter dat zijn gegevens bijna zeker gelekt zijn bij een datalek bij zijn oude energieleverancier NLE eind 2019. De leverancier geeft ook toe dat het zou kunnen dat zijn gegevens ook bij het datalek zaten, maar hij is daar nooit over bericht.  Meneer heeft hier ook melding van gemaakt bij de AP, omdat het voor meer mensen zou kunnen gelden, maar hier nooit iets op terug gehoord. Wat is de reactie van de AP hierop? Is er onderzoek gedaan naar het datalek bij energieleverancier NLE in 2019 en of er meer betrokkenen zijn die niet door NLE zijn geïnformeerd hierover?**

·         De AP doet geen mededelingen over individuele gevallen van datalekken. Dat zou wel kunnen als we bijvoorbeeld onderzoek hebben gedaan, zover zijn dat we conclusies trekken of bijvoorbeeld handhaven.

·         We krijgen veel klachten en tips over dit soort lekken. De AP kijkt dan na of het datalek wel of niet gemeld is.

·         De AP heeft niet de capaciteit om overal onderzoek naar te doen.

·         En het pijnlijke verhaal is dat wij de tienduizenden mensen die jaarlijks een klacht indienen bij de AP, door capaciteitsgebrek niet snel genoeg kunnen helpen, en vaak ook niet in de mate die wij wensen.

·         Wij moeten mensen helaas vertellen dat het zes maanden duurt voordat we hun klacht kunnen oppakken. En dus wachten er bijna 10.000 mensen totdat de AP hun klacht kan behandelen.

·         Dat capaciteitsgebrek staat ook in de Tweede Kamer hoog op de agenda: de Kamer nam met grote meerderheid een motie aan voor meer budget bij de AP. Het volgend kabinet buigt zich over die kwestie.

**Verantwoordelijkheid bedrijven/ organisaties**

* Bedrijven/organisaties hebben een grote verantwoordelijkheid in de bescherming van persoonsgegevens.
* Als klant vertrouw jij je waardevolle persoonsgegevens toe aan een bedrijf of organisatie..
* Dan moet jij er vanuit kunnen gaan dat dat bedrijf alles doet om je gegevens goed te beschermen.
* Zeker als het gevoelige gegevens van heel veel mensen beheert.

**Waarom moeten organisaties een datalek melden bij de AP?**

* Het is essentieel dat een organisatie een datalek direct bij de AP meldt.
* De AP kan die organisatie helpen de schade voor de getroffen mensen te beperken.
* Door aanwijzingen te geven hoe het lek snel te dichten.
* Door het bedrijf op te dragen snel de slachtoffers van het lek te informeren.
* Door toekomstige datalekken helpen voorkomen.
* Meld een bedrijf een datalek niet of te laat, dan kan de AP daar een forse boete voor opleggen.

**Datalek op tijd melden**

* Organisaties met een datalek moeten dat melden bij de AP via het [meldloket datalekken](https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0). De AP merkt dat organisaties lang niet alle datalekken melden die zij zouden moeten melden. Dat wordt bijvoorbeeld duidelijk als slachtoffers een klacht of tip bij de AP achterlaten.
* Dat is ernstig, want als mensen niet weten dat hun gegevens mogelijk in het bezit zijn van criminelen, kunnen zij geen maatregelen treffen. Zoals hun wachtwoord wijzigen of hun creditcard blokkeren. De schade kan dan flink oplopen.
* Op dit moment heeft de AP 9 onderzoeken lopen naar datalekken die niet of niet op tijd zijn gemeld. Organisaties die een datalek niet (op tijd) melden bij de AP, zijn in overtreding en kunnen een boete krijgen.

**Nemen datadiefstallen toe?**

* We zien een explosieve toename van datadiefstal van maar liefst 30% in 2020.
* Door tekort aan personeel en budget bij de AP krijgen datalekken te weinig opvolging: van de 27.000 datalekken in 2019 leidt maar 0,3% tot onderzoek en 0,15% over totaal van  2020. Dat is een halvering.

**Wat moet je doen als je gegevens bij een datalek zijn betrokken?**

Krijg je bericht van je bank of je telecombedrijf dat jouw persoonsgegevens zijn getroffen door een datalek? Kijk dan goed wat er is precies is gelekt over jou. Zijn bijvoorbeeld je e-mailadres en wachtwoord gelekt? Verander dan voor de zekerheid je wachtwoord. Als je hetzelfde wachtwoord gebruikt op verschillende websites, verander deze dan ook. Wees daarnaast extra alert op e-mails, WhatsApp-berichtjes of telefoontjes waarbij iemand zegt je te contacteren namens een organisatie en bijvoorbeeld vraagt om bepaalde gegevens door te geven of op een bepaalde link te klikken te sturen. Word je opeens gebeld, gewhatsappt of gemaild door bijvoorbeeld je bank of je telecombedrijf? Check altijd of je ook daadwerkelijk met je bank of telecombedrijf te maken hebt. Bijvoorbeeld door het gesprek te beëindigen en zelf je bank of telecombedrijf op te bellen.

**Identiteitsfraude**

Een van de risico's na een datalek is identiteitsfraude. Bij identiteitsfraude maken criminelen misbruik van jouw gegevens. Bijvoorbeeld door op jouw naam spullen te kopen zonder te betalen, of een lening of telefoonabonnement af te sluiten. Houd dus in de gaten of je vreemde dingen ziet gebeuren op je bankrekening, en of je vreemde mailtjes ziet binnenkomen over aankopen die jij helemaal niet hebt gedaan.

Vermoed je dat je slachtoffer bent van identiteitsfraude? Onderneem dan actie. In [deze folder](https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/documenten/publicaties/2015/12/02/geef-oplichters-geen-kans-een-veilig-id) lees je wat jij precies kunt doen, tegen verschillende vormen van identiteitsfraude.

**Moet je extra waakzaam zijn voor phishing mail? Zo ja, waar herken je dat aan?**

Criminelen worden steeds beter in het namaken van websites en e-mails van organisaties. Het is dus belangrijk om goed te kijken wat er in zo’n mailtje staat. Komt het e-mailadres overeen met de naam van het bedrijf? Wat staat er achter het @-teken? Staat in de aanhef ‘Geachte meneer/mevrouw’ of gebruiken ze daadwerkelijk jouw naam? Vragen ze je om op een link te klikken om je gegevens ‘aan te vullen’ of ‘te controleren’? Dit zijn allemaal aanwijzingen aan de hand waarvan je kan controleren of een bericht ook daadwerkelijk van een organisatie komt en ook ‘echte’ is. Vertrouw je het niet? Bel dan altijd naar de organisatie of ga zelf naar de website van de organisatie en klik niet zomaar op een link.

**Ook bankrekeningnummers zijn gelekt, moet ik nu mijn bank bellen?**

Nee, maar wees alert op berichten per e-mail, WhatsApp of telefoon waarbij mensen informatie proberen te ontfutselen, zoals je pincode of informatie op je identiteitskaart. Jouw bank zal je nooit per telefoon, e-mail, WhatsApp of sms om een bepaalde code vragen of vragen je bankpas te versturen naar een bepaald adres. Twijfel je over de identiteit van de afzender, hang dan op, verwijder het bericht en/of contacteer je bank. Let ook op eventuele afschrijvingen van je bankrekening. Criminelen kunnen je bijvoorbeeld je bankrekening gebruiken om spullen met jouw bankrekeningnummer te kopen. Kijk voor meer info ook op [www.veiligbankieren.nl](http://www.veiligbankieren.nl).

**Is het nodig om wachtwoorden en dergelijke te veranderen?**

Bedrijven verplicht zijn om je persoonsgegevens, zoals je wachtwoorden, veilig te bewaren. Toch is het verstandig om je wachtwoord voor de zekerheid te wijzigen als je een bericht ontvangt van een bedrijf dat ze getroffen zijn door een datalek waarbij wachtwoorden zijn getroffen. Als je een wachtwoord gebruikt voor andere websites loop je ook het risico dat criminelen de gelekte gegevens gebruiken om in te breken in accounts bij andere bedrijven. Gebruik daarom ook niet overal hetzelfde wachtwoord.

**Hoe kan je voorkomen dat jouw gegevens in de toekomst weer bij een datalek betrokken raken?**

Organisaties zijn verantwoordelijk voor het goed beveiligen van jouw persoonsgegevens, maar elke ketting is zo sterk als zijn zwakste schakel. Je kan organisaties, die jouw persoonsgegevens verwerken, helpen door niet overal hetzelfde wachtwoord te gebruiken. Daarbij kan je gebruikmaken van een wachtwoordmanager die niet alleen je wachtwoorden bewaard, maar ook sterke wachtwoorden voor je kan generen. Biedt een organisatie ook een zogenaamde een tweede factorbeveiliging aan, bijvoorbeeld door ook een code te vragen die je per sms of een speciale app ontvangt als je wil inloggen, maak daar dan ook gebruik van. Tot slot: wees kritisch naar wie er om je gegevens vraagt en op welke manier. Klik niet zomaar op een link als je het niet vertrouwt, maar ga zelf naar de website van de organisatie.

**Welke voorzorgsmaatregelen kun je zelf nemen om je online privacy (in het algemeen) te waarborgen?**

Wees zelf de baas over jouw data. Vraagt een bedrijf om gegevens die het helemaal niet nodig heeft om jou een dienst te leveren? Geef ze dan niet. En maak gebruik van je [privacyrechten](https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten). Jij hebt het recht op antwoord op je vragen over jouw data. Als jij daarom vraagt, dan [moet een bedrijf vertellen welke data het over jou heeft verzameld](https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/recht-op-inzage). En als jij daarom vraagt, dan [moet een bedrijf in de meeste gevallen jouw persoonsgegevens wissen](https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/recht-op-vergetelheid). Zo heb je nog veel meer rechten wat betreft je eigen persoonsgegevens. Zo houd je de controle over jouw persoonsgegevens. Als jij zorgt dat bedrijven niet onnodig persoonsgegevens van jou op hun servers hebben staan, is de kans dat jouw gegevens op straat liggen bij een datalek natuurlijk kleiner.