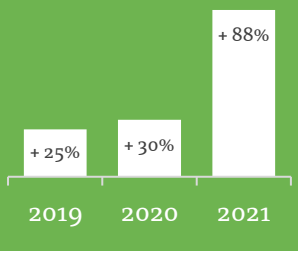
AUTORITEIT
PERSOONSGEGEVENS

Datalekkenrapportage 2021

Stijging meldingen cyberaanvallen 2021	Trend procentuele stijging meldingen cyberaanvallen	Aantal datalekmeldingen 2021
↑ 88%		24.866

Introductie

In 2021 ontving de Autoriteit Persoonsgegevens (AP) 24.866 datalekmeldingen. Dat is een stijging van 4% ten opzichte van 2020 (23.976 datalekmeldingen).

Het aantal meldingen van datalekken door hacking, malware of phishing (hierna: cyberaanvallen) is opnieuw fors gestegen. In 2021 waren er 88% meer van deze meldingen dan in 2020. Ook in 2020 en 2019 was er een stijging, respectievelijk van 30% en 25% ten opzichte van het voorgaande jaar. Het aantal cyberaanvallen omvat dit jaar 9% van het totaal aantal datalekmeldingen, vorig jaar was dit nog maar 5% van het aantal datalekmeldingen.

De AP maakt zich zorgen over de blijvende stijging van het aantal gemelde cyberaanvallen. Vooral IT-leveranciers, die persoonsgegevens van veel mensen verwerken, lijken doelwit te zijn van cyberaanvallen. Op basis van datalekmeldingen schat de AP in dat cyberaanvallen bij IT-leveranciers het afgelopen jaar minimaal 7 miljoen slachtoffers hebben gemaakt. In deze rapportage besteedt de AP daarom extra aandacht aan cyberaanvallen bij IT-leveranciers. Verder gaat de AP nader in op het toezicht op de meldplicht datalekken.

Exponentiële stijging cyberaanvallen

In 2021 ontving de AP 2.210 datalekmeldingen als gevolg van cyberaanvallen. Dat meer organisaties een cyberaanval bij de AP hebben gemeld dan de voorgaande jaren, komt voor een deel doordat de AP nadrukkelijker is gaan sturen op de meldplicht van organisaties bij grote cyberaanvallen. Binnen deze sterkte stijging is een trend zichtbaar: criminelen richten zich steeds vaker op IT-leveranciers. Die leveren bijvoorbeeld softwarediensten, digitale werkplekken of opslagruimte aan organisaties. Dat leidt tot een

clustering van persoonsgegevens op de servers van IT-leveranciers. Daardoor zijn zij een gewild doelwit voor criminelen: er valt veel te halen.

De AP ziet drie soorten cyberaanvallen: hacking-, malware- en phishingaanvallen. Malware is kwaadaardige software, waarvan ransomware een bekend voorbeeld is. Ransomware versleutelt data van gebruikers. Dit heeft tot gevolg dat een organisatie haar data niet meer kan openen. Verder kunnen criminelen de versleutelde data hebben gekopieerd naar een door hen beheerde plek, buiten het netwerk van de getroffen partij. Meestal eisen criminelen losgeld in ruil voor de sleutel om de data te ontsleutelen. Het afgelopen jaar zag de AP steeds vaker dat criminelen niet-betalende organisaties extra onder druk zetten door een deel van de gestolen data te koop aan te bieden op het *dark web*. Daarbij ging het vaak om zeer gevoelige informatie, zoals paspoortkopieën.

Losgeld betalen bij ransomware: geen reden om slachtoffers niet te informeren

De AP merkt op dat sommige organisaties de slachtoffers niet informeren als zij getroffen zijn door een ransomwareaanval. Als reden geven deze organisaties aan dat zij losgeld hebben betaald aan criminelen. Zij denken dat zij daarmee hebben voorkomen dat de criminelen de persoonsgegevens verder verspreiden. Die toezegging hebben zij ook gekregen van de criminelen.

Deze redenering klopt echter niet. Een ransomwareaanval vormt een inbreuk op zowel de vertrouwelijkheid als de beschikbaarheid van persoonsgegevens. De criminelen voeren ransomwareaanvallen vooral uit voor het geld. Daarom is er geen enkele garantie dat zij de gegevens ook daadwerkelijk verwijderen en nooit zullen doorverkopen, ook al hebben zij al losgeld gekregen.

De AP ziet het betalen van losgeld niet als een passende achteraf genomen maatregel in de zin van artikel 34 van de Algemene verordening gegevensbescherming (hierna: AVG) om slachtoffers niet te informeren over een ransomwareaanval.

Datalekken door ransomware altijd melden aan AP en slachtoffers

Datalekken door ransomware kunnen grote risico's opleveren voor de slachtoffers. Daarom moeten dit soort datalekken vrijwel altijd gemeld worden aan de AP en aan de slachtoffers.

De gestolen persoonsgegevens kunnen misbruikt worden om gerichte phishingaanvallen te plegen op deze slachtoffers. Daarbij sturen de criminelen - ogenschijnlijk uit naam van de getroffen organisatie - een mail naar de slachtoffers om geld of meer informatie afhandig te maken. Daarnaast kunnen de gestolen persoonsgegevens worden toegevoegd aan bestaande datasets, die bijvoorbeeld verkocht worden op het dark web. Deze gegevens worden dan uiteindelijk gebruikt in spamlijsten of in bruteforceaanvallen, waarbij met eerder gelekte informatie geprobeerd wordt om toegang te krijgen tot gebruikersaccounts bij andere organisaties, zoals banken, webshops of bestuursorganen.

Datalekken bij IT-leveranciers

De AP heeft het afgelopen jaar 28 datalekken gezien bij IT-leveranciers. De impact hiervan is enorm. Deze 28 datalekken hebben geleid tot 1.800 datalekmeldingen bij de AP. Hierbij zijn naar schatting minimaal 7 miljoen slachtoffers getroffen. Omdat niet alle datalekken aan de AP worden gemeld, zijn dit er waarschijnlijk nog veel meer. De meeste datalekken bij IT-leveranciers worden veroorzaakt door cyberaanvallen. In het cybersecuritybeeld 2021 signaleren de NCTV en het NCSC dat cyberaanvallen het zenuwstelsel van de maatschappij aantasten.[1] Eén cyberaanval bij een grote IT-leverancier heeft een schokeffect op de hele distributieketen.[2] De AP heeft 14 van deze datalekken bij IT-leveranciers onderzocht.

Voorbeeld van een datalek bij een IT-leverancier

Een verloskundigenpraktijk (de verwerkingsverantwoordelijke) schakelt een IT-dienstverlener (de verwerker) in, die een standaardapplicatie levert om patiënt- en personeelsdossiers aan te maken en op te slaan. Deze IT-dienstverlener is een grote speler in deze specifieke markt en levert deze dienst ook aan veel andere verloskundigenpraktijken in Nederland.

De IT-dienstverlener wordt getroffen door een ransomwareaanval. Hierdoor zijn patiënt- en personeelsgegevens van de verloskundigenpraktijken versleuteld en gekopieerd door criminelen. De criminelen verwijderen alle back-ups, waardoor de persoonsgegevens niet meer beschikbaar zijn voor de verloskundigenpraktijken. De criminelen eisen losgeld van de IT-leverancier en dreigen anders de patiënt- en personeelsgegevens te publiceren op het dark web.

[1] Cybersecuritybeeld Nederland 2021, p. 7. Zie: https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.
[2] Cyberaanvallen op IT-leveranciers worden ook wel 'supply chain attacks' genoemd.

Organisaties (AVG: verwerkingsverantwoordelijken) besteden hun IT-diensten vaak uit aan een IT-leverancier (AVG: verwerker). Denk bijvoorbeeld aan het faciliteren van digitale werkplekken, het leveren van op maat gemaakte software en de opslag van data. Een cyberaanval op die IT-leverancier kan dan ook meerdere organisaties treffen die gebruikmaken van de IT-diensten. Uiteindelijk kan één cyberaanval grote groepen mensen treffen van wie organisaties persoonsgegevens verwerken. IT-leveranciers lijken een aantrekkelijk doelwit te zijn: criminelen kunnen een grote hoeveelheid persoonsgegevens gebruiken om de IT-leverancier af te persen.

Bedrijfsprocessen zijn tegenwoordig sterk afhankelijk van digitale processen. Grootschalige cyberincidenten hebben daarom een enorme impact op de bedrijfsvoering van organisaties. Bedrijfsprocessen worden door zulke incidenten ernstig belemmerd of moeten zelfs worden stilgelegd. En persoonsgegevens kunnen op straat komen te liggen. Zo kan een ransomwareaanval op een winkel of een IT-leverancier tot gevolg hebben dat bepaalde producten niet meer verkocht kunnen worden.

De AP ziet dat de prioriteit bij getroffen organisaties vaak ligt bij het herstellen van de processen. Daarnaast is het echter belangrijk dat zij de slachtoffers van het cyberincident zo snel mogelijk informeren. Zo kunnen slachtoffers zichzelf beschermen tegen de gevolgen van het datalek. Bijvoorbeeld door hun wachtwoord te veranderen of extra alert te zijn op phishingmails.

Toezicht door de AP: sturen op meldplicht bij verwerkingsverantwoordelijken

Bij een cyberaanval bij een verwerker, zoals een IT-leverancier, is het belangrijk dat de slachtoffers zo snel mogelijk worden geïnformeerd en dat de klanten van de verwerker (de verwerkingsverantwoordelijken) binnen 72 uur een datalekmelding doen bij de AP. Op basis van datalekmeldingen kan de AP de aard en de omvang van grootschalige cyberaanvallen monitoren en toezicht houden op de meldplicht aan de slachtoffers en de te treffen beveiligingsmaatregelen.

De AP kan ervoor kiezen om de verwerker direct na een cyberaanval te wijzen op de verplichting om alle opdrachtgevers volledig te informeren over de cyberaanval. De opdrachtgever heeft als verwerkingsverantwoordelijke een meldplicht aan de AP en aan de slachtoffers. De AP merkt dat de meldplicht beter wordt nageleefd na interventie van de AP.

Daarnaast kan de AP een onderzoek starten naar de meldplicht aan de AP en de slachtoffers en/of de getroffen beveiligingsmaatregelen.

Verplichtingen van IT-dienstverleners

De meldplicht datalekken (artikel 33 en 34 van de AVG) geldt in eerste instantie voor verwerkingsverantwoordelijken. Maakt een verwerkingsverantwoordelijke gebruik van de IT-diensten van een verwerker? Dan blijft de verwerkingsverantwoordelijke verantwoordelijk voor de verwerking van persoonsgegevens en dus ook voor de melding van een datalek aan de AP én aan de slachtoffers. De verwerker is verplicht om de verwerkingsverantwoordelijke zo snel mogelijk te informeren over een

datalek (artikel 33, tweede lid van de AVG). Verder is de verwerker verplicht om de verwerkingsverantwoordelijke te helpen bij een datalek (artikel 28, derde lid, onder f van de AVG). Het is dus belangrijk dat IT-leveranciers snel, transparant en volledig communiceren naar de verwerkingsverantwoordelijken bij een datalek. Verwerkingsverantwoordelijken moeten immers de kans krijgen om zo snel mogelijk te beoordelen of zij het datalek moeten melden aan de slachtoffers en aan de AP. En zij moeten ook bepalen welke maatregelen zij zelf moeten nemen om het datalek te beëindigen en/of de negatieve gevolgen te beperken.

De AP constateert echter dat IT-leveranciers vaak niet snel, transparant en volledig genoeg communiceren naar de verwerkingsverantwoordelijken. De oorzaken verschillen. Zo willen IT-leveranciers soms wachten tot een uitgebreid onderzoek naar het datalek is afgerond. Of zijn zij bang voor reputatieschade en onrust bij hun klanten. Dit zijn voor de AP geen goede redenen. IT-leveranciers spelen een belangrijke rol in de meldplicht aan de slachtoffers en de meldplicht aan de AP door de verwerkingsverantwoordelijke. Wanneer IT-leveranciers de verwerkingsverantwoordelijken niet direct en volledig informeren, kan dat ertoe leiden dat IT-leveranciers de AVG overtreden

Praktisch – een datalek bij een verwerker melden bij de AP

Op onze website staat wie wat moet melden bij een datalek bij een verwerker. De AP verwacht van iedere verwerkingsverantwoordelijke een aparte datalekmelding. Daarmee kan de AP de specifieke feiten en omstandigheden vaststellen per verwerkingsverantwoordelijke. Bovendien kan de AP uitsluitend de verwerkingsverantwoordelijke aanspreken, niet de verwerker, als de slachtoffers van een datalek ten onrechte niet worden geïnformeerd.

Zes aanbevelingen voor organisaties

Besteedt u als organisaties (een deel van) uw ICT uit aan een of meerdere IT-leveranciers? Dan kunt u zelf maatregelen treffen om de impact van een datalek bij uw IT-leverancier(s) te verkleinen. Daarnaast kunt u vooraf maatregelen nemen om ervoor te zorgen dat u de meldplicht datalekken adequaat kunt naleven.

De AP heeft hiervoor zes aanbevelingen:

1. Schakel alleen IT-leveranciers in die **genoeg garanties geven voor passende technische en organisatorische** beveiligingsmaatregelen. U kunt daarbij letten op eventuele certificering van de IT-leverancier. Let op: u blijft als verwerkingsverantwoordelijke volgens de AVG verantwoordelijk voor de beveiliging van persoonsgegevens, ook als u de beveiliging volledig aan de IT-leverancier heeft uitbesteed.
2. Pas **dataminimalisatie** toe en controleer de naleving. De AP ziet nog te vaak dat bij cyberaanvallen gegevens worden getroffen waarvan de bewaartermijn is overschreden en die dus al gewist hadden moeten zijn.
3. Leg in de **verwerkersovereenkomst** concrete afspraken vast over de hulp die de IT-leverancier geeft bij naleving van de meldplicht datalekken. In de verwerkersovereenkomst maakt u afspraken over het verwerken van persoonsgegevens en de beveiliging daarvan.
4. **Controleer periodiek** of de IT-leverancier de verwerkersovereenkomst naleeft.
5. Maak een **actieplan melding datalekken** om de termijnen na te leven. De AVG vereist snel handelen. De IT-leverancier moet u zo snel mogelijk informeren over een datalek. U moet het

datalek vervolgens binnen 72 uur nadat u hiervan op de hoogte bent geraakt, melden bij de AP. De slachtoffers moet u direct informeren.

6. Zorg voor een zorgvuldig opgesteld en **goed bijgehouden verwerkingsregister**, zowel bij uzelf als bij de verwerker. Het verwerkingsregister helpt u een snelle inschatting te maken welke organisaties en categorieën van persoonsgegevens zijn geraakt bij een datalek. Zo wordt het eenvoudiger om de gevolgen voor de slachtoffers in kaart te brengen.

Toezicht AP op de meldplicht datalekken

Het toezicht van de AP is risicogestuurd. Dat betekent dat de AP zich voornamelijk richt op die datalekken die de grootste risico's opleveren voor de slachtoffers. De AP identificeert risico's aan de hand van datalekmeldingen en dataleksignalen. Een signaal kan bijvoorbeeld een bericht in de media zijn. De AP kan een risico vaststellen op een omstandigheid uit één datalekmelding, maar ook op trends die volgen uit meerdere datalekmeldingen.

Naast de al genoemde stijging van 88% van het aantal gemelde cyberaanvallen identificeert de AP onder andere risico's bij datalekken:

- waarbij slachtoffers ten onrechte niet worden geïnformeerd over het datalek;
- bij verwerkers, met name IT-leveranciers;
- met grote aantallen slachtoffers;
- met bijzondere en/of gevoelige persoonsgegevens;
- die ten onrechte niet aan de AP worden gemeld.

Verder staan in het toezicht van de AP op de meldplicht datalekken de slachtoffers centraal. Een belangrijk aandachtspunt hierbij is ervoor zorgen dat verwerkingsverantwoordelijken slachtoffers adequaat informeren over een datalek. Zodat de slachtoffers ook zelf maatregelen kunnen nemen om de impact te beperken. Bijvoorbeeld door het wachtwoord van een account te veranderen, alerter te zijn op bankafschrijvingen en andere online applicaties.

Risicogestuurd toezicht op de meldplicht datalekken

De bijna 25.000 datalekmeldingen in 2021 hebben geleid tot 36 onderzoeken. De intensiteit van toezicht neemt toe, naarmate de AP grotere risico's identificeert. Dat betekent dat de AP niet elke datalekmelding even intensief onderzoekt.

Monitoring: bijna 18.000 meldingen
Bij een groot deel van de datalekmeldingen verricht de AP na een eerste beoordeling geen verdere toezichtshandelingen. Van zulke meldingen ontving de AP er bijna 18.000 in 2021.

Verdiepend toezicht: ruim 7.000 meldingen
Het afgelopen jaar heeft de AP in 7.000 datalekmeldingen extra toezichtshandelingen verricht. Deze extra toezichtshandelingen waren noodzakelijk omdat in deze datalekmeldingen door de AP grote risico's werden geïdentificeerd. Bijvoorbeeld omdat het ging om veel slachtoffers of (veel) gevoelige persoonsgegevens. Bij deze meldingen doet de AP een diepgaandere controle.

Wat doet de AP tijdens het verdiepend toezicht?
Tijdens zo'n nadere controle kan de AP contact opnemen met de meldende organisatie om vragen te stellen over het datalek. Bijvoorbeeld omdat de datalekmelding onduidelijk is, onregelmatigheden bevat of inconsistent is. Daarnaast kan de AP na een dergelijke controle een normoverdragende brief sturen of een normoverdragend gesprek voeren. In zo'n brief of gesprek wijst de AP de organisatie op de regels. Zoals de meldplicht aan de slachtoffers of de norm voor mobiele datadragers met gevoelige en/of bijzondere persoonsgegevens.

De AP neemt niet bij elke melding contact op met de verwerkingsverantwoordelijke. Bijvoorbeeld omdat uit de melding volgt dat al voldoende nieuwe beveiligingsmaatregelen zijn getroffen en alle betrokkenen al zijn geïnformeerd.

Onderzoeken naar aanleiding van datalekmeldingen
In 2021 is de AP naar aanleiding van 36 datalekmeldingen een onderzoek gestart. Deze 36 datalekmeldingen brachten naar het oordeel van de AP de grootste risico's voor de slachtoffers met zich mee. Het ging voornamelijk om situaties waarbij een verwerkingsverantwoordelijke de slachtoffers van een ransomwareaanval ten onrechte niet informeerde. En om situaties waarbij een verwerkingsverantwoordelijke onvoldoende nieuwe beveiligingsmaatregelen had genomen om nieuwe datalekken te voorkomen.

Van de 36 onderzoeken waren 14 onderzoeken gericht op IT-leveranciers. De andere 22 onderzoeken waren gericht op diverse organisaties, zoals zorginstellingen en overheden.

Een onderzoek kan zich richten op een enkele organisatie maar ook op een groep organisaties. Bijvoorbeeld naar aanleiding van een cyberaanval bij een IT-leverancier. Deze onderzoeken kunnen leiden tot een boete, maar dat hoeft niet altijd. Per situatie weegt de AP af hoe ze het effectiefst kan optreden. Hierbij houdt de AP ook rekening met al lopende onderzoeken.

De AP heeft te weinig middelen om bij elke datalekmelding met zeer ernstige risico's een onderzoek te starten.

Handhaving door de AP: boete Transavia

De AP kan organisaties die de AVG overtreden een boete opleggen. In 2021 heeft de AP een boete opgelegd van 400.000 euro aan luchtvaartmaatschappij Transavia, vanwege het slecht beveiligen van persoonsgegevens. Door die slechte beveiliging kon een hacker in 2019 de systemen van Transavia binnendringen. Het wachtwoord was te eenvoudig te raden, meerfactorauthenticatie ontbrak, autorisaties waren te uitgebreid en systemen waren onvoldoende van elkaar gescheiden. Daarbij had de hacker toegang tot systemen waarin hij gegevens van 25 miljoen mensen had kunnen inzien. Vastgesteld is dat de hacker persoonsgegevens van zo'n 83.000 personen downloadde.

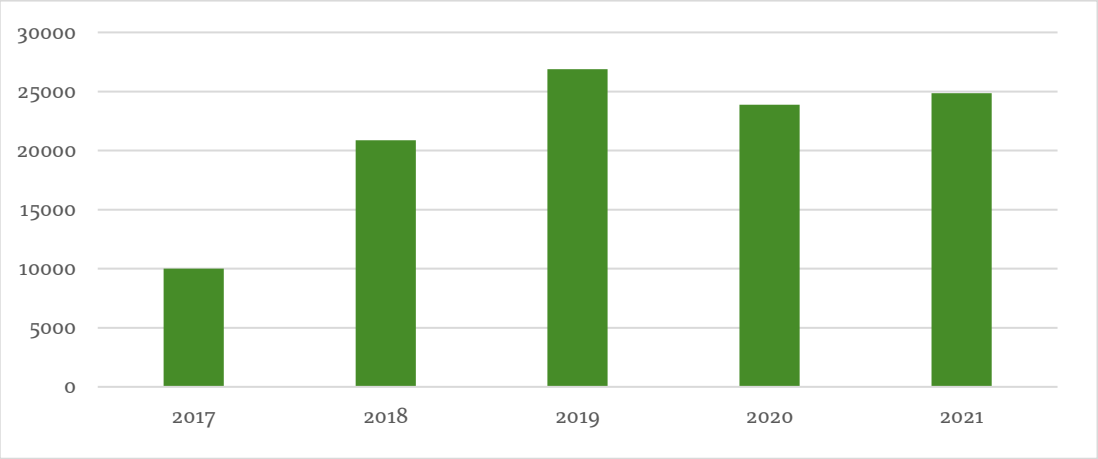
Verder legde de AP in 2021 een boete op aan Booking.com omdat het bedrijf een datalek te laat had gemeld, aan PVV Overijssel omdat de partij een datalek niet had gemeld en aan het OLVG omdat dit ziekenhuis persoonsgegevens slecht beveiligde.

Overzicht feiten en cijfers 2021

Aantal datalekmeldingen

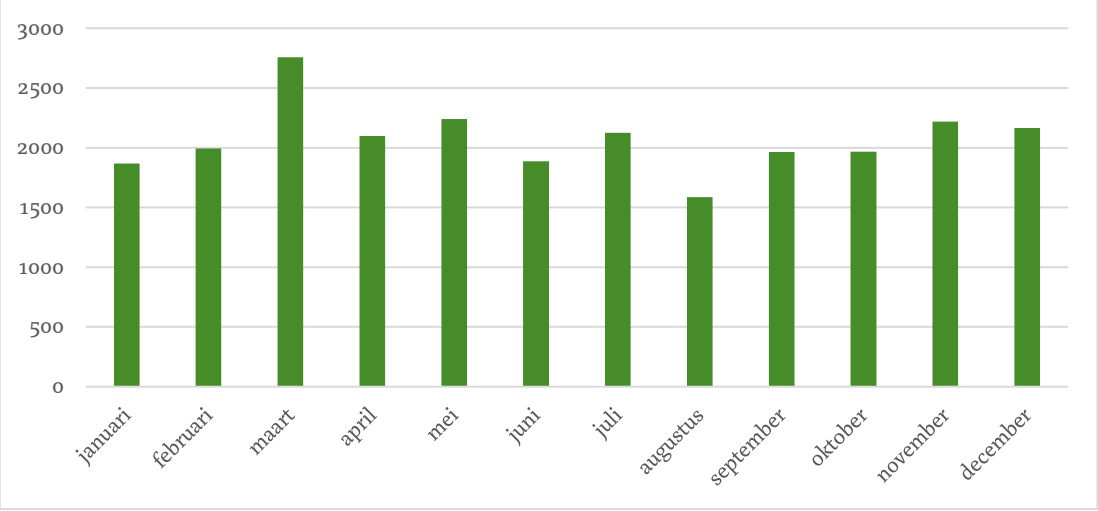
Nederland staat in de top drie van landen in Europa waar de meeste datalekken worden gemeld. Doordat Nederland sterk gedigitaliseerd is, is het risico op (grote/ernstige) datalekken hier relatief hoog. Daardoor is extra aandacht vereist voor de bescherming van persoonsgegevens en cybersecurity.

Onderstaande grafiek laat het verloop van het aantal datalekmeldingen sinds 2017 zien:



Totaal aantal datalekmeldingen ontvangen door de AP 2017-2021

Onderstaande grafiek toont het aantal ontvangen datalekmeldingen per maand in 2021. In maart 2021 vond er een datalek plaats bij een IT-leverancier met veel datalekmeldingen van verwerkingsverantwoordelijken tot gevolg.

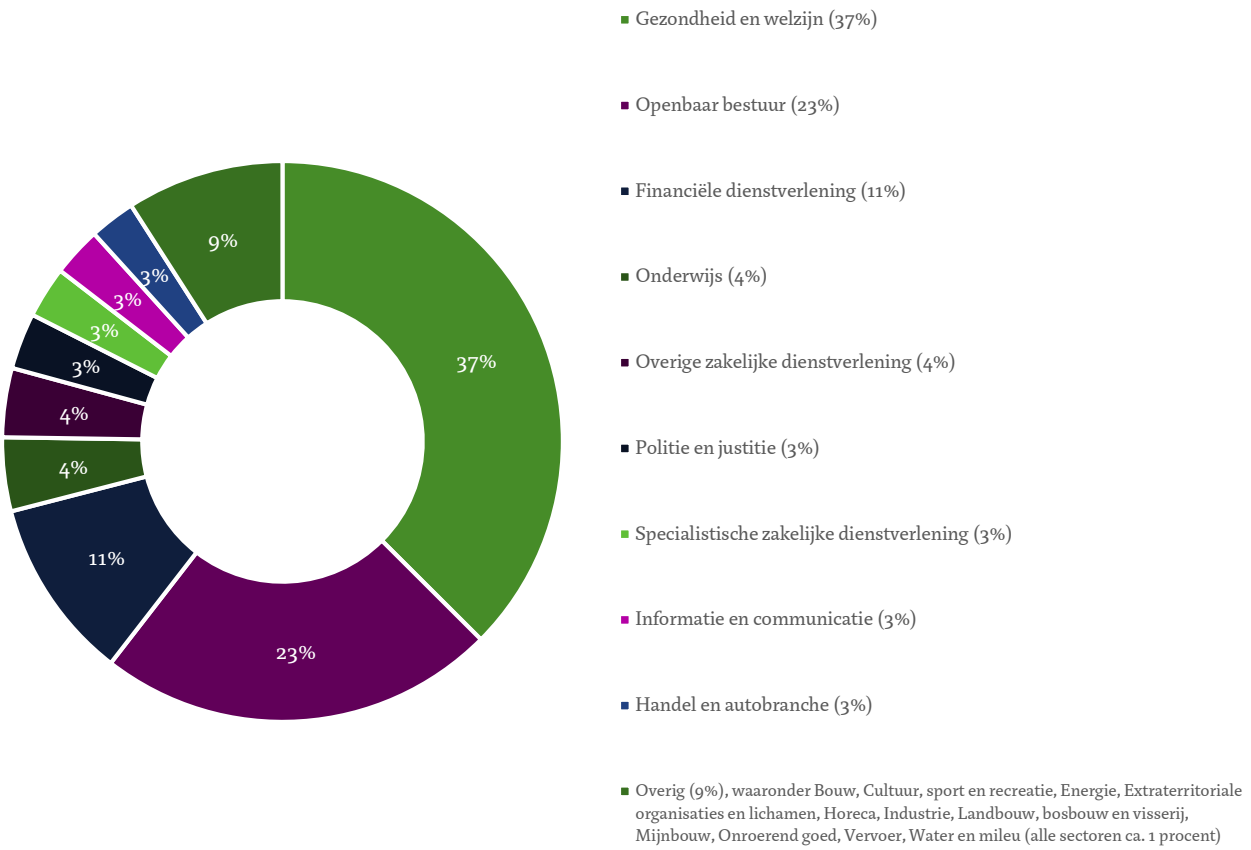


Totaal aantal datalekmeldingen per maand ontvangen door de AP in 2021

Aantal grensoverschrijdende datalekmeldingen

De 24.866 meldingen zijn meldingen van datalekken die de AP in Nederland heeft ontvangen via het meldloket datalekken op de website van de AP. Daarnaast hebben andere Europese privacytoezichthouders in 47 gevallen een grensoverschrijdend datalek gedeeld met de AP. Dat gebeurt bijvoorbeeld als een datalek bij een andere Europese toezichthouder is gemeld, maar het mogelijk ook significante gevolgen heeft voor slachtoffers in Nederland. De AP deelt in voorkomende gevallen ook meldingen over grensoverschrijdende datalekken met andere privacytoezichthouders, bijvoorbeeld ter informatiedeling. Dit deed de AP in 2021 elf keer.

Aantal datalekmeldingen per sector



De meeste datalekmeldingen kwamen in 2021 uit de sector gezondheid en welzijn (37%), gevolgd door openbaar bestuur (23%) en financiële dienstverlening (11%). Binnen deze top 3 is het aantal meldingen uit de sector financiële dienstverlening gedaald met 51% ten opzichte van 2020, uit de sector gezondheid en welzijn gestegen met 29% en uit de sector openbaar bestuur gestegen met 9%.

De daling in de financiële sector komt voornamelijk doordat één organisatie (een incassokantoor) drastisch minder is gaan melden. Deze organisatie blijkt een werkproces te hebben aangepast, waardoor er veel minder datalekken ontstaan. Er zijn namelijk veel minder betalingsherinneringen bij verkeerde ontvangers terechtgekomen.

Type datalekken

Het aantal datalekken waarbij persoonsgegevens bij een verkeerde ontvanger terechtkomen, blijft net als afgelopen jaren hoog. De AP vraagt nu expliciet aan organisaties of het gaat om datalekken per brief of per e-mail. Daarbij valt op dat veruit de meeste datalekken ontstaan bij per post bezorgde persoonsgegevens. De voornaamste reden waarom dit incident optreedt, is dat de geadresseerde niet langer op het geregistreerde adres woont.

De categorie 'Hacking, malware en/of phishing' omvat 9% van het totaal aantal meldingen. Vorig jaar was dit nog maar 5% van het totaal aantal meldingen.