AUTORITEIT
PERSOONSGEGEVENS

Meldplicht datalekken: facts & figures
Overzicht feiten en cijfers 2019

Aantal meldingen	Stijging totaal aantal meldingen	Stijging meldingen hacking & malware	Sector met meeste gemelde datalekken
26.956	↑ 29% ten opzichte van 2018	↑ 25% ten opzichte van 2018	Financiële sector

Introductie

Stijging aantal meldingen hacking, phishing of malware-incidenten

In 2019 ontving de Autoriteit Persoonsgegevens (AP) bijna 27.000 datalekmeldingen. Dat is een stijging van 29% ten opzichte van 2018. De AP ontving dit jaar een kwart meer meldingen naar aanleiding van hacking, phishing of malware-incidenten dan in het jaar daarvoor. Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken hier doelwit van.

Thema: openbaar bestuur

De AP legt de komende jaren in het toezichtwerk extra nadruk op een aantal focusgebieden[1] waaronder de digitale overheid. Centrale en lokale overheden beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens, zoals Burgerservicenummers en gegevens over zorg en maatschappelijke dienstverlening. Het gaat met name om wettelijke en/of onvrijwillige verwerking van gegevens en burgers kunnen niet terecht bij een alternatieve dienstverlener. Datalekken in deze sector kunnen daarom grote impact hebben op burgers.

Ook staat sinds de invoering van de meldplicht datalekken de sector openbaar bestuur samen met de sector zorg en de financiële sector steevast in de top 3 van sectoren met de meeste meldingen. We lichten de sector openbaar bestuur er daarom dit keer uit. In 2019 ontving de AP 4.624 datalekmeldingen uit de sector openbaar bestuur. Dit zijn 27% meer meldingen dan in 2018.

[1] De drie focusgebieden van de AP voor 2020-2023 zijn datahandel, Digitale Overheid en Artificiële Intelligentie & algoritmes.

Cijfers 2019

Aantal meldingen

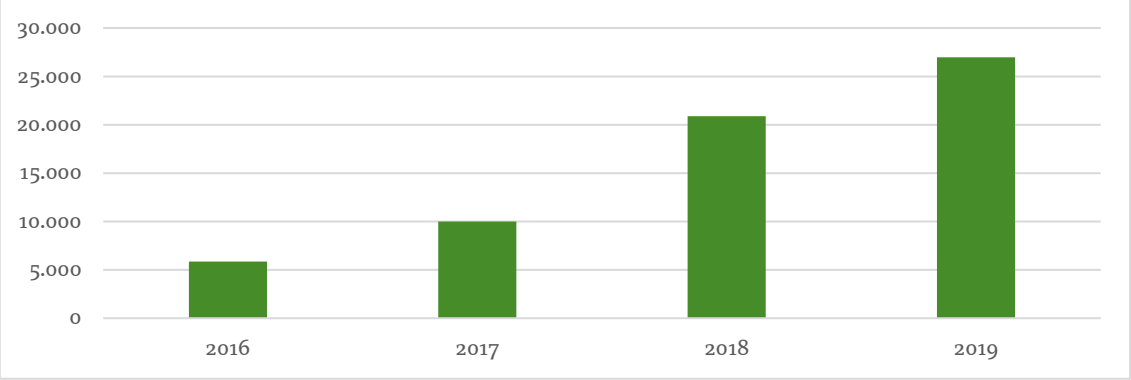
Nederland behoort tot de drie koplopers van landen in Europa waar de meeste datalekken worden gemeld, naast Duitsland en het Verenigd Koninkrijk. Daarnaast worden in Nederland per inwoner de meeste datalekken gemeld van alle landen in Europa. Naast de stijging in het totale aantal meldingen viel op dat de AP in 2019 25% procent meer meldingen ontving over hacking, phishing en/of malware-incidenten dan in 2018. Om het gestegen aantal datalekmeldingen grondig te kunnen onderzoeken zal de capaciteit van de AP moeten groeien.

Gemiddeld ontving de AP in 2019 ongeveer 2.200 meldingen per maand. De eerste 9 maanden van 2019 bleef het aantal meldingen dat de AP ontving stabiel rond de 2.000 meldingen per maand. In de laatste drie maanden van 2019 steeg het aantal datalekmeldingen sterk. In oktober ontving de AP 2.600 meldingen, in november 3.100, en in december 3.600 meldingen.
Deze stijging werd onder andere veroorzaakt door een toename in het aantal datalekmeldingen afkomstig van factoring bureaus. Dit zijn bureaus die uitstaande facturen van organisaties opkopen en overnemen. Bij deze meldingen ging het met name om datalekken als gevolg van herinneringsbrieven voor openstaande facturen die zijn ingezien door een verkeerde ontvanger. Mede door de stijging in het aantal meldingen van factoring bureaus was de sector Financieel in 2019 de sector met de meeste gemelde datalekken.

Bewustwording

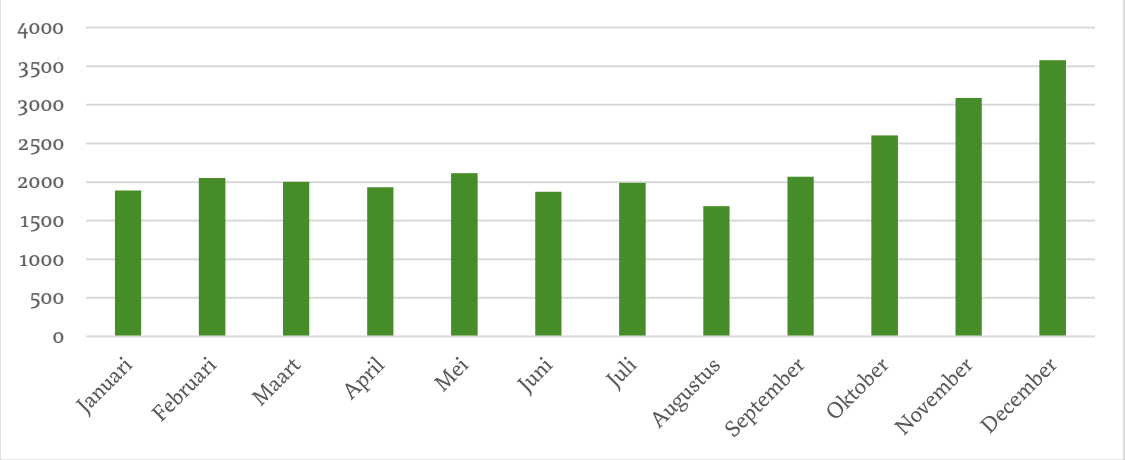
De afgelopen twee jaar is er veel aandacht geweest voor de AVG en zijn door veel organisaties, waaronder de AP, interne en externe bewustwordingscampagnes gestart. Organisaties in Nederland lijken zich mede hierdoor steeds meer bewust te worden van de meldplicht datalekken. Een andere mogelijke verklaring voor het hoge aantal meldingen is dat in Nederland al een meldplicht datalekken geldt sinds 1 januari 2016, tweeëneenhalf jaar eerder dan in andere Europese landen. Daarnaast loopt Nederland binnen de EU voorop op het gebied van digitalisering. Daardoor is het risico op (grote/ernstige) datalekken in Nederland relatief hoog. De hoge mate van digitalisering van de Nederlandse maatschappij vereist extra aandacht voor fundamentele vraagstukken als privacy bescherming en cybersecurity.

Onderstaande grafiek laat de toename van het aantal datalekmeldingen sinds 2016 zien:



Totaal aantal datalekmeldingen ontvangen door de AP 2016-2019

Deze grafiek toont het aantal ontvangen meldingen per maand in 2019.



Totaal aantal datalekmeldingen per maand ontvangen door de AP in 2019

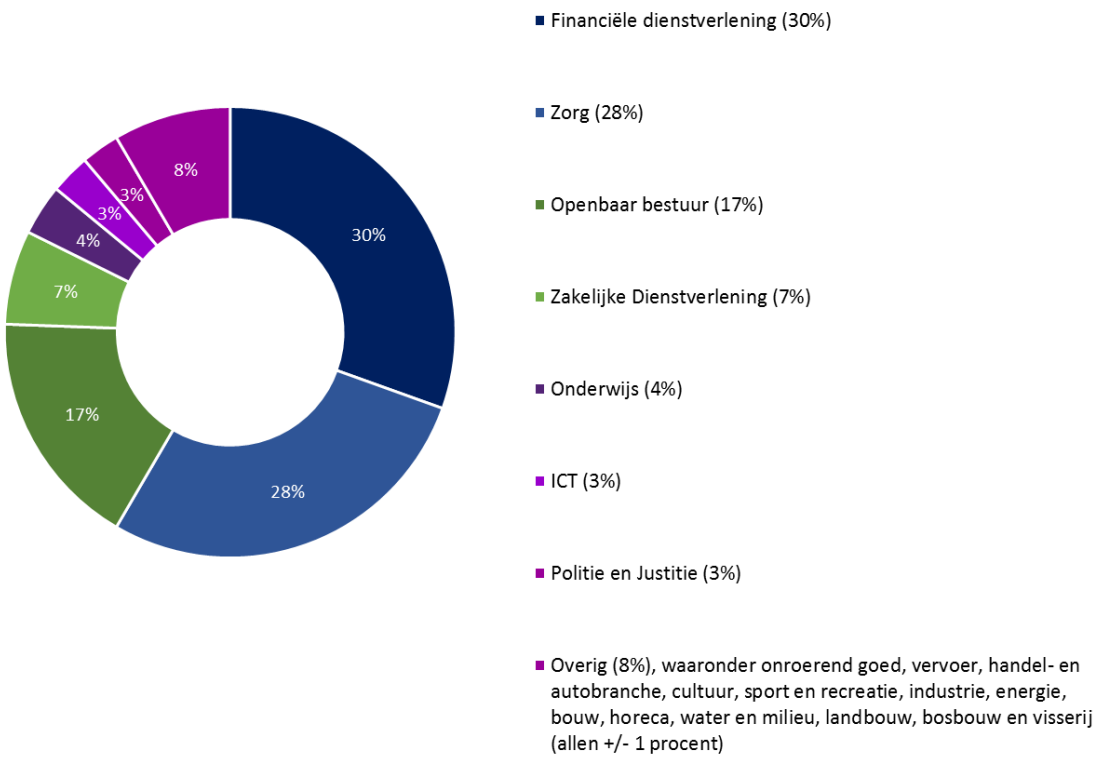
Grensoverschrijdende datalekken

De 26.956 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 toezichthouders in 75 gevallen een grensoverschrijdend datalek gedeeld met de AP. Dat gebeurt bijvoorbeeld als een datalek bij een andere Europese toezichthouder is gemeld, maar het datalek (mogelijk) ook gevolgen heeft voor betrokkenen in meerdere lidstaten waaronder personen in Nederland. De AP deelt ook meldingen over grensoverschrijdende datalekken met andere toezichthouders. Dit was bijvoorbeeld het geval bij een melding van een grote verzekeringsmaatschappij, over een mogelijk datalek waarbij een gegevensdrager met daarop persoonsgegevens van een grote groep klanten uit meerdere landen uit een kluis is gestolen. Verschillende Europese privacytoezichthouders zijn bij deze zaak betrokken.

Campagne met praktische informatie over datalekken

In het kader van de campagne 'Wat betekent de privacywet voor jou(w) bedrijf?' heeft de AP in juli 2019 de informatie over datalekken op haar website uitgebreid. Bestaande Q&A zijn aangepast, er zijn nieuwe Q&A toegevoegd en de AP biedt praktische hulpmiddelen om de naleving makkelijker te maken. Op de website hulpbijprivacy.nl staan tips over wat te doen bij een datalek, en tips over hoe datalekken kunnen worden voorkomen.

Meldingen datalekken per sector



De meeste datalekken zijn gemeld vanuit de financiële sector (30%), de zorgsector (28%) en de sector openbaar bestuur (17%). Dit zijn ook de sectoren waarvan de AP in voorgaande jaren het grootste aantal datalekmeldingen ontving. Binnen deze top 3 is het aantal meldingen in de financiële sector ten opzichte van 2018 gestegen met 53%, het aantal meldingen in de zorgsector gestegen met 23% en het aantal meldingen in de sector openbaar bestuur gestegen met 27%.

Financiële sector

Het grootste aantal datalekken binnen de financiële sector wordt gemeld door factoring bureaus (71%). Daarbij gaat het meestal om een herinneringsbrief voor een openstaande factuur die geopend retour komt. Na factoring bureaus zijn de meeste meldingen binnen de financiële sector afkomstig van financiële instellingen, zoals banken, (11%), en van verzekeringsmaatschappijen en pensioenfondsen (10%).

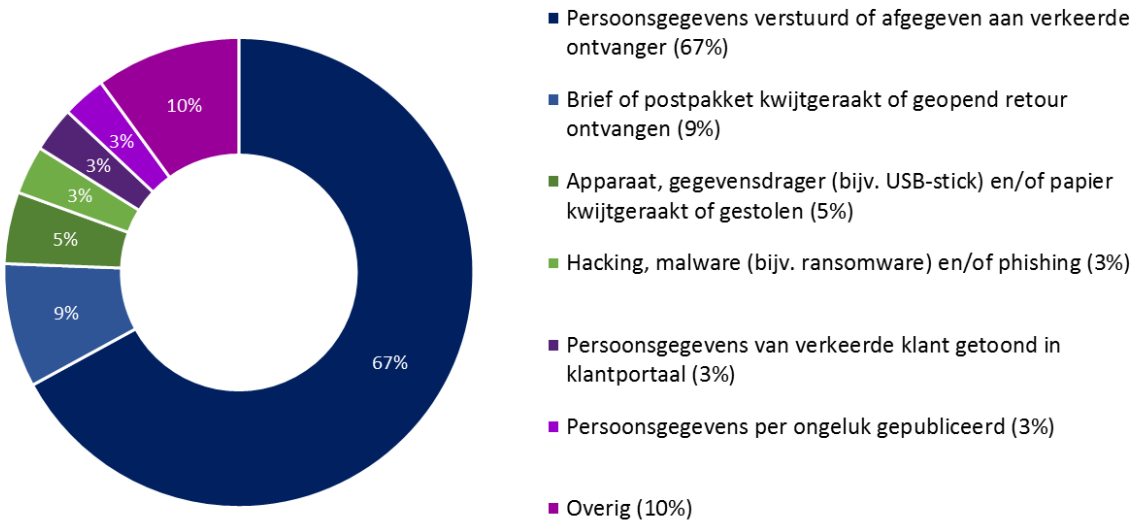
Zorg

Het grootste aantal datalekmeldingen binnen de zorgsector is afkomstig van ziekenhuizen (25%), apotheken (20%) en stichtingen die bevolkingsonderzoek uitvoeren (9%).

Openbaar bestuur

Binnen de sector openbaar bestuur worden de meeste datalekken gemeld door zelfstandige bestuursorganen (38%), gevolgd door gemeenten (33%) en de Rijksoverheid (25%). Een uitgebreidere analyse van de datalekmeldingen door de sector openbaar bestuur is opgenomen in het laatste deel van deze rapportage.

Type datalekken



Versturen of afgeven van persoonsgegevens aan verkeerder ontvanger

In 2019 steeg het aantal meldingen maar bleven de percentages van het type datalekken in grote lijnen hetzelfde ten opzichte van 2018. In meer dan de helft van de gevallen (67%) gaat het datalek om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Dit was ook het meest gemelde type datalek in 2018 (eveneens 63%) en in 2017 (47%). Bij dit type datalek kan het gaan om een e-mail met daarin gevoelige persoonsgegevens die wordt verzonden naar de verkeerde ontvanger. Bijvoorbeeld door een typefout of omdat er in het e-mailprogramma een verkeerde geadresseerde wordt geselecteerd. Daarnaast komt het voor dat personen hun eigen gegevens opvragen bij organisaties, maar door een administratieve fout vervolgens ook persoonsgegevens van anderen ontvangen.

Datalekken met post

In 9% van de gevallen gaat het om poststukken met gevoelige gegevens die bij de verkeerde persoon terechtkomen en geopend retour worden gestuurd. De onjuiste ontvanger heeft dan kennis kunnen nemen van de inhoud van de brief. Dit soort datalekken komt het meeste voor in de zorgsector (44%), zakelijke dienstverlening (16%) en openbaar bestuur en politie en justitie (beiden 14%).

Datalekken met mobiele apparatuur

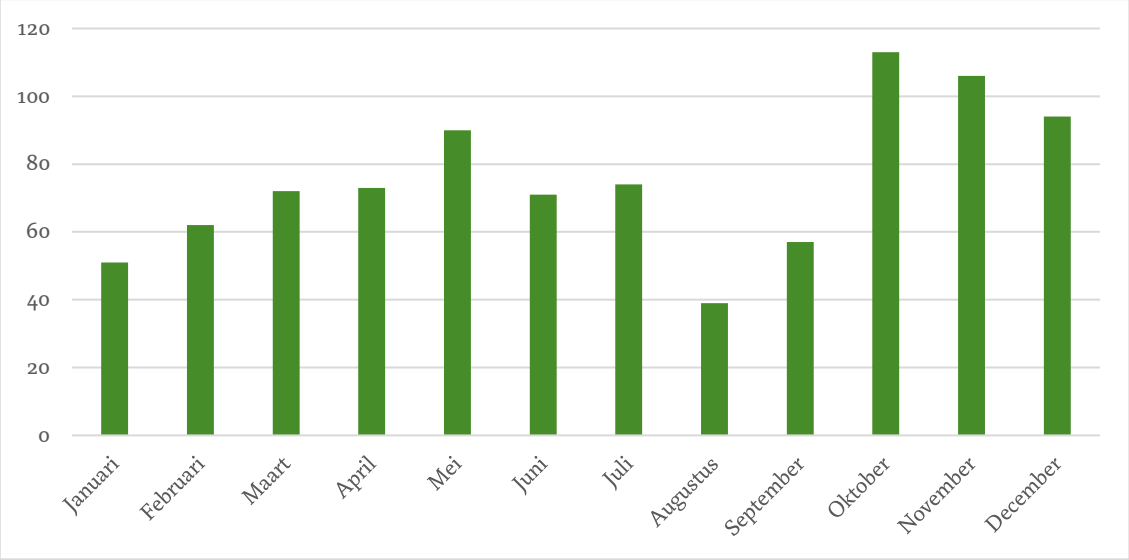
Het komt ook voor dat mobiele apparaten of gegevensdragers zoals laptops, tablets, smartphones en USB-sticks waarop persoonsgegevens zijn opgeslagen, kwijtraken of worden gestolen. Dit type datalek komt het meest voor in de sector zorg (27%), gevolgd door de sector openbaar bestuur (19%) en de sectoren onderwijs en informatie en communicatie (beiden 11%).

Datalekken door hacking, malware en/of phishing

In 2019 ontving de AP 902 meldingen over hacking, malware[2] en/of phishing[3]-incidenten. Dit is een stijging van 25% ten opzichte van 2018. Dit type datalek komt het meest voor in de sector zakelijke dienstverlening (14%) gevolgd door de sectoren zorg en onderwijs (beiden 13%), de sector ICT-dienstverlening (11%), en de sector handel en autobranche (8%). Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken doelwit van hacking, malware en/of phishing. Van de 902 meldingen die de AP in 2019 ontving over hacking, malware en/of phishing-incidenten, werden in 30% van de gevallen meer dan 500 personen getroffen. In de laatste drie maanden van 2019 was een sterke stijging waarneembaar in het aantal meldingen over hacking, malware en/of phishing.

[2] Malware is kwaadaardige software. Een bekend voorbeeld van malware is 'ransomware'. Dit is 'gijzelsoftware' die een computer of bestanden gijzelt. Meestal wordt daarna betaling geëist, bijvoorbeeld via prepaidkaarten of Bitcoin. Besmetting verloopt vaak via besmette bestanden, zoals een e-mailbijlage of via advertenties op internet die een lek in niet-geüpdatete software misbruiken.
[3] Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben informatie van mensen te ontfutselen. Een bekend voorbeeld van phishing is het oplichten van mensen door ze te lokken naar een valse website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor onderschept de fraudeur/hacker de gegevens.

Dit is weergegeven in onderstaande tabel:



Aantal datalekmeldingen (hacking, malware en/of phishing) ontvangen door de AP per maand in 2019

Rapport Cybersecuritybeeld Nederland 2019

Uit het rapport Cybersecuritybeeld Nederland 2019 (CSBN), opgesteld door de Nationaal Coördinator Terrorismebestrijding (NCTV) en het Nationaal Cyber Security Centrum (NCSC), blijkt dat cybercriminelen in 2019 veelvuldig misbruik hebben gemaakt van de Nederlandse digitale infrastructuur. Eenvoudige aanvalsmiddelen, zoals phishing, of misbruik van gebruikersnamen en wachtwoorden zijn daarbij effectief gebleken. Mogelijk heeft dit bijgedragen aan de stijging in het aantal meldingen over hacking, malware en/of phishing-incidenten die de AP in 2019 ontving.

Risico's bij hacking, malware en/of phishing

Datalekken door hacking, malware en/of phishing leveren over het algemeen een hoog risico op voor de betrokkenen. Ook wanneer er alleen namen en e-mailadressen zijn getroffen. Deze gegevens kunnen door de hacker namelijk misbruikt worden voor het uitvoeren van nieuwe spam- en phishing-aanvallen. Vaak kan alleen na het uitvoeren van digitaal forensisch onderzoek vastgesteld worden wat welke persoonsgegevens zijn getroffen door het datalek, en wat er met deze gegevens is gebeurd. Zo kan je er bij een ransomware-aanval niet vanuit gaan dat gegevens alleen versleuteld zijn. Mogelijk zijn de gegevens ook gekopieerd, vernietigd of gewijzigd door de hacker. Om de gevolgen voor de betrokkenen goed in te kunnen schatten is daarom aanvullend onderzoek nodig.

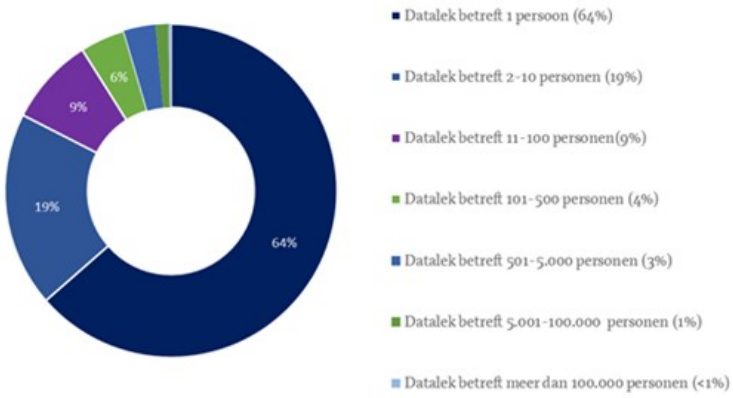
De AP raadt aan om altijd direct een melding te doen wanneer persoonsgegevens (mogelijk) zijn getroffen als gevolg van een hacking, malware en/of phishing-aanval. De gevolgen zullen bij zo'n aanval namelijk niet meteen duidelijk zijn.

TIP: Datalekken door hacking, malware en/of phishing altijd melden
Datalekken door hacking, malware en/of phishing kunnen grote risico's opleveren voor de betrokkenen. Houd er rekening mee dat dit soort datalekken over het algemeen gemeld moeten worden aan de AP en aan de betrokkenen. Meld dit soort incidenten altijd op tijd (binnen 72 uur na ontdekking). Wanneer u het incident direct meldt kan de AP controleren of u de risico's van het incident goed heeft ingeschat. En kan de AP, indien nodig, direct contact met u opnemen over het datalek.

Gegevens over de gezondheid zijn over het algemeen zeer gevoelig. Wanneer dit soort gegevens wordt ingezien door onbevoegden zal er over het algemeen sprake zijn van een hoog risico voor de betrokkenen. Ook wanneer de onjuiste ontvanger deze gegevens nadat ze zijn ingezien vernietigt of terugstuurt. Er heeft dan namelijk al een grote inbreuk plaatsgevonden op de privacy van de betrokkene. Ook datalekken met Burgerservicenummers leveren over het algemeen een hoog risico op, met name wanneer daarnaast ook nog aanvullende persoonsgegevens zijn gelekt. Wanneer het BSN in combinatie met andere persoonsgegevens in handen komt van onbevoegden kunnen de betrokkenen een risico lopen op (identiteits-)fraude. Hetzelfde geldt voor datalekken met kopieën van paspoorten en legitimatiebewijzen.

TIP: Gevoelige gegevens
Medische gegevens en Burgerservicenummers zijn gevoelig. Houd er rekening mee dat dit soort datalekken gemeld moeten worden aan de AP en aan de betrokkenen.

Maximum aantal betrokkenen



Meestal 1 persoon betrokken

In de ruime meerderheid van de in 2019 gemelde datalekken, namelijk 64%, raakte het datalek 1 persoon. In 2018 was dit percentage nog 58%. In 2019 zijn dus vaker kleinere datalekken gemeld. Het gaat in deze

gevallen meestal om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Bij 400 meldingen (1,5%) heeft het datalek een zeer groot aantal betrokkenen getroffen (5.000 of meer personen). Deze grotere datalekken werden in 2019, net als in 2018, vooral veroorzaakt door hacking, malware en/of phishing, namelijk in 30% van de gevallen.

Niet gemelde en te laat gemelde datalekken

De AP merkt dat, net zoals in 2018, niet alle meldplichtige datalekken door organisaties worden gemeld. Dat wordt bijvoorbeeld duidelijk als betrokkenen bij de AP een klacht of melding achterlaten over een (meldplichtig) datalek, terwijl dat door de organisatie zelf niet is gemeld.

In 2019 zijn 5 onderzoeken afgerond in zaken waarbij (mogelijk) een meldplichtig datalek niet is gemeld aan de AP. Deze onderzoeken kunnen leiden tot een sanctie. Daarnaast zijn in 2019 10 onderzoeken naar niet gemelde datalekken afgerond die leidden tot een alternatieve interventie door de AP, zoals een normuitleggend gesprek of een waarschuwende brief. 15 onderzoeken zijn nog lopend.

Belang van de meldplicht aan de AP en aan betrokkenen

De meldplicht stelt de AP onder meer in staat om te controleren of er adequaat op de inbreuk is gereageerd, of de inbreuk is beëindigd, of de genomen of aangekondigde beveiligingsmaatregelen voldoende zijn om nieuwe inbreuken te voorkomen, en of de personen die zijn getroffen door het datalek moeten worden geïnformeerd, en zo ja, of de organisatie dat heeft gedaan of nog gaat doen. Met de meldplicht aan de betrokkene is beoogd de betrokkene op de hoogte te stellen van wat er met diens gegevens is gebeurd, en de consequenties die dat voor zijn belangen heeft. Hierdoor kan de getroffen persoon, voor zover dat mogelijk is, zich tegen de gevolgen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen.

Te laat gemelde datalekken

De AP merkt dat niet alle meldplichtige datalekken door organisaties op tijd worden gemeld. Dat wordt bijvoorbeeld duidelijk wanneer uit een melding blijkt dat de organisatie al langer dan 72 uur op de hoogte was van het datalek. Of wanneer uit een tip of klacht blijkt dat de organisatie al eerder op de hoogte was. De AP beschouwt dit als een ernstige zaak.

In 2019 zijn twee onderzoeken afgerond naar aanleiding van een te laat gemeld datalek. Deze onderzoeken kunnen leiden tot een sanctie. Daarnaast is in 2019 één onderzoek afgerond die leidde tot een alternatieve interventie door de AP. Twee onderzoeken zijn nog lopend.

Belang van op tijd melden aan de AP

U dient een meldplichtig datalek, voor zover mogelijk, te melden binnen 72 uur nadat u het datalek ontdekt heeft. Het is belangrijk dat u een datalek op tijd meldt. Soms lopen betrokkenen als gevolg van een datalek direct risico op schade. Dan is het belangrijk dat betrokkenen zo snel mogelijk worden gewaarschuwd en dat er onmiddellijk maatregelen worden genomen om de gevolgen van het datalek te beperken. Door op tijd te melden stelt u de AP in de gelegenheid om snel in te grijpen, indien uit de melding blijkt dat het besluit om betrokkenen niet te informeren niet correct is, bijvoorbeeld, omdat de risico's van het datalek worden onderschat. Of wanneer uit de melding blijkt dat u onvoldoende maatregelen heeft genomen om de gevolgen van het datalek te beperken of om nieuwe datalekken te voorkomen. Door tijdig te melden kan de AP dus snel ingrijpen wanneer dat nodig is. Daardoor worden de betrokkenen beter beschermd.

Acties AP

Bij 1.180 datalekmeldingen heeft de AP naar aanleiding van de melding actie ondernomen richting de organisatie die het datalek gemeld had. Daarbij ging het om verschillende soorten acties:

- In 79% van de gevallen is telefonisch contact opgenomen met de meldende organisatie om aanvullende vragen te stellen over het datalek,
- In 4% van de gevallen is schriftelijk contact opgenomen met de meldende organisatie om aanvullende informatie op te vragen over het datalek,
- In 10% van de gevallen is een normuitleggende brief gestuurd,
- In 5% van de gevallen is een gesprek gevoerd met de organisatie, waarbij op de privacyregels wordt gewezen en zo nodig op maatregelen wordt aangedrongen,
- Daarnaast lopen er momenteel meerdere onderzoeken naar aanleiding van te laat gemelde en niet-gemelde datalekken (zie pagina 9.).

Naast datalekmeldingen ontvangt de AP ook klachten en signalen die betrekking hebben op datalekken. Naar aanleiding hiervan zijn nog circa 70 acties ondernomen richting de organisaties waar het datalek plaatsvond. Ook lopen momenteel drie onderzoeken naar aanleiding van datalekken die het gevolg waren van gebrekkige beveiliging. Deze onderzoeken kunnen leiden tot een sanctie. In juli 2019 heeft de AP een onderzoek afgerond bij het HagaZiekenhuis en een boete opgelegd van 460.000 euro voor het onvoldoende beveiligen van persoonsgegevens.

Haga beboet voor onvoldoende interne beveiliging patiëntendossiers

In juli 2019 rondde de AP een onderzoek af bij het HagaZiekenhuis. Uit dat onderzoek bleek dat het ziekenhuis de interne beveiliging van patiëntendossiers niet op orde had. De AP heeft het HagaZiekenhuis voor de onvoldoende beveiliging een boete opgelegd van 460.000 euro.

Wat doet de AP met een datalekmelding?

Wanneer uit uw melding blijkt dat de meldplicht goed is nageleefd en voldoende maatregelen zijn genomen krijgt de meldende organisatie geen reactie. Als de AP inhoudelijke vragen heeft over de melding neemt de AP in de meeste gevallen binnen 2 weken contact met u op.

Acties naar aanleiding van een datalekmelding
Afhankelijk van de situatie kan de AP besluiten het volgende te doen na ontvangst van een melding van een datalek :

- u bellen voor meer informatie over het datalek;
- u bellen om u extra uitleg en advies te geven;
- een inlichtingenverzoek doen. Bijvoorbeeld om het rapport van uw onderzoek naar het datalek op te vragen;
- u een brief sturen met extra uitleg over de normen en hoe te handelen bij datalekken;
- u verplichten om de betrokken personen te informeren wanneer u dat onterecht niet heeft gedaan;
- een onderzoek starten bij een mogelijke overtreding van de meldplicht. Bijvoorbeeld wanneer u een datalek niet heeft gemeld aan de AP. Of te laat heeft gemeld.
- een diepgaand onderzoek starten. Bijvoorbeeld naar het naleven van de verplichting om passende maatregelen te nemen om persoonsgegevens te beveiligen.
- de melding sluiten. Wanneer uit uw melding blijkt dat u de meldplicht goed heeft nageleefd en voldoende maatregelen zijn genomen om nieuwe inbreuken te voorkomen.

AUTORITEIT
PERSOONSGEGEVENS

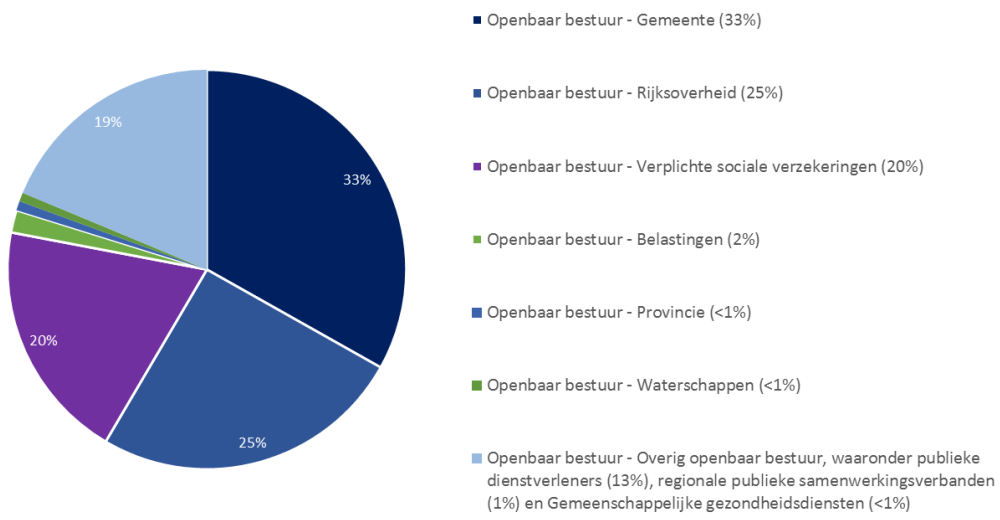
Meldplicht datalekken facts & figures
Openbaar bestuur

Aantal meldingen 2019	Top 3 organisaties die het meest melden	Meest voorkomende inbreuk
4.624	1. Gemeenten 2. Rijksoverheid 3. Verplichte soc. verzekeringen	70% persoonsgegevens verstuurd aan verkeerde ontvanger

Aantal meldingen openbaar bestuur

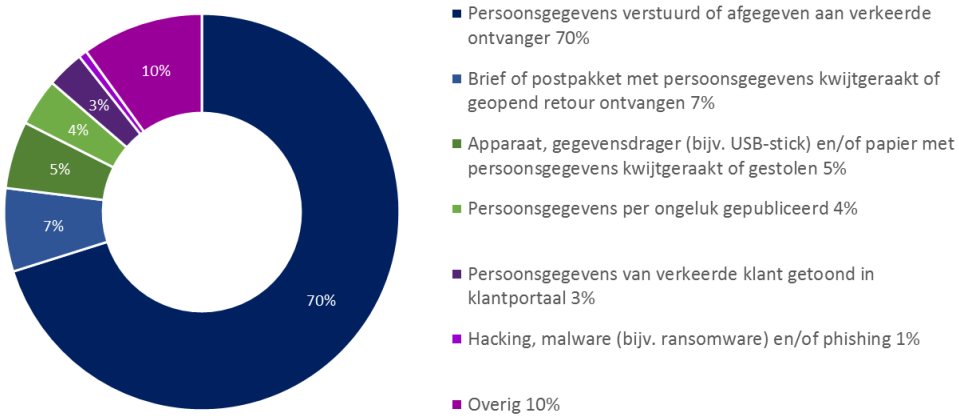
In 2019 ontving de AP 4.624 datalekmeldingen afkomstig van de sector openbaar bestuur, een toename van 27% ten opzichte van 2018 (3.630 meldingen).

Meldingen datalekken in de sector openbaar bestuur



Binnen de sector openbaar bestuur worden de meeste datalekken gemeld door gemeenten (33%), gevolgd door de Rijksoverheid (25%) en verplichte sociale verzekeringen (20%). In 2018 meldden gemeenten ook de meeste datalekken in deze sector (39%). Bij de meeste meldingen in de sector openbaar bestuur ging het om een datalek met één betrokkene (59%). In 33 gevallen (1%) ging het om een datalek met 5.000 of meer betrokkenen.

Type datalekken in de sector openbaar bestuur



Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

Bij alle subsectoren van de sector openbaar bestuur, met uitzondering van de subsector belastingen, komt het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger, verreweg het meeste voor. Dit type datalek komt met name voor bij gemeenten (27%) en bij de Rijksoverheid (25%). In veel gevallen gaat het om het om datalekken als het gevolg van het gebruik van verouderde adressen, of de verwisseling van klant/relatienummers, waardoor klanten de verkeerde brief ontvangen. Daarnaast gaat het vaak om incidenten waarbij per ongeluk meerdere brieven aan verschillende personen in één envelop zijn gestopt of dubbelzijdig zijn geprint.

TIP : Veilig e-mailen
De AP merkt dat sommige gemeenten gevoelige persoonsgegevens, zoals gegevens over (jeugd)zorg of WMO, onbeveiligd e-mailen naar externe partijen. Door menselijke fouten kunnen deze gegevens bij een verkeerde ontvanger terecht komen, bijvoorbeeld door een typefout in het e-mailadres, of door een verkeerde geadresseerde aan te klikken. Dit soort incidenten kan voorkomen worden door de gevoelige gegevens als bijlage op te nemen in het e-mailbericht en deze bijlage te versleutelen met een wachtwoord. Of door de communicatie via een beveiligd portaal te laten verlopen.

Datalekken met post

In 7% van de datalekmeldingen in de sector openbaar bestuur gaat het om een brief of postpakket dat is kwijtgeraakt, of geopend retour ontvangen. Dit gebeurt in de meeste gevallen (41%) bij gemeenten. Deze datalekken kunnen betrekking hebben op gevoelige persoonsgegevens van kwetsbare groepen. Het kunnen bijvoorbeeld brieven zijn die gaan over de wijziging, beëindiging of toewijzing van een sociale voorziening. Zoals Jeugdzorg of WMO, of gemeentelijke schuldhulpverlening. Wanneer deze brieven worden ingezien door onbevoegden kan dat grote impact hebben op de persoonlijke levenssfeer van de betrokkene.

Voorbeeld datalek: inzage persoonsgegevens van collega's

Een deurwaarderskantoor stuurt een brief over een medewerker per ongeluk naar de afdeling waar die medewerker werkzaam is. In de brief legt het deurwaarderskantoor beslag op het loon van de medewerker. De brief bevat gevoelige gegevens over de financiële positie van de medewerker. Deze brief was bedoeld voor de HR afdeling van het bestuursorgaan. De medewerker van de afdeling die de brief ten onrechte had ontvangen heeft de brief opengemaakt en daarbij inzage gekregen in de gegevens van diens collega.

Het bestuursorgaan meldt het datalek bij de AP. In de melding geeft het bestuursorgaan aan de betrokken medewerker niet te informeren over het datalek. Als reden geeft het bestuursorgaan aan dat de collega die de brief heeft geopend zorgvuldig met de gegevens om zal gaan, omdat hij gebonden is aan een ambtelijke geheimhoudingsplicht. Daardoor zouden de risico´s voor de betrokken medewerker te verwaarlozen zijn. De AP stuurt naar aanleiding van de datalekmelding een brief aan het bestuursorgaan waarin het bestuursorgaan wordt opgedragen om de betrokkene alsnog onmiddellijk te informeren, aangezien het datalek kan leiden tot reputatieschade. Omdat het hier gevoelige persoonsgegevens van een directe collega van de onjuiste ontvanger betrof, is het niet relevant dat de onjuiste ontvanger gehouden is aan de ambtelijke geheimhoudingsplicht. Deze geheimhoudingsplicht is gericht op de vertrouwelijke omgang met persoonsgegevens van externen (burgers). Dat de medewerker een eed heeft afgelegd om zorgvuldig met gegevens om te gaan doet echter niets af aan de inbreuk op de persoonlijke levenssfeer van de collega. Het bestuursorgaan dient naar aanleiding van de brief van de AP een vervolgmelding in waarin zij aangeeft de betrokken medewerker via een persoonlijk bericht te informeren over het incident. De AP sluit het dossier.

Datalekken met mobiele apparatuur

Datalekken als gevolg van verloren of gestolen mobiele apparatuur met daarop persoonsgegevens komen binnen de sector openbaar bestuur het meest voor bij de Rijksoverheid (58%) en bij gemeenten (31%). Vaak gaat het hierbij om incidenten waarbij een (werk)laptop of telefoon wordt gestolen uit een geparkeerde auto. Daarnaast komt het voor dat mobiele apparatuur wordt verloren doordat ze worden vergeten in het openbaar vervoer.

TIP: Versleutelen

Soms ontvangt de AP meldingen van organisaties die bijzondere persoonsgegevens, bijvoorbeeld medische gegevens, zonder versleuteling opslaan op werklaptops. Een datalek kan dan plaatsvinden omdat de laptop wordt gestolen. De laptop alleen beveiligen met een wachtwoord is niet genoeg.

Versleutelen (encryptie) zorgt ervoor dat de gegevens gecodeerd worden op basis van een bepaald algoritme. De versleuteling zorgt ervoor dat derden niet de gegevens kunnen lezen wanneer ze niet beschikken over de toegepaste code (de sleutel).

Wanneer u draagbare apparatuur gebruikt, zoals tablets, telefoons, laptops of USB-sticks, zorg dan dat gevoelige en/of bijzondere persoonsgegevens, zoals medische gegevens, altijd versleuteld zijn opgeslagen. Zo beperkt u de risico's voor de betrokkenen, wanneer u een draagbaar apparaat verliest of wanneer deze wordt gestolen.

Datalekken door hacking, malware en/of phishing

In de sectoren openbaar bestuur worden datalekken door hacking, malware en/of phishing het meest gemeld door gemeenten (60%), gevolgd door provincies (16%). Meestal gaat het bij deze meldingen over phishing. De AP heeft geen meldingen ontvangen afkomstig uit de sector openbaar bestuur over (geslaagde) ransomware-aanvallen. Een mogelijke verklaring hiervoor is dat organisaties in deze sector over het algemeen een hoog volwassenheidsniveau hebben op het gebied van databeveiliging. Daardoor kan malware, waaronder ransomware, minder makkelijk systemen besmetten.

Phishing bij gemeenten

De AP heeft in 2019 meerdere datalekmeldingen ontvangen van gemeenten die getroffen zijn door phishing. Gemeenten zijn relatief grote organisaties met veel medewerkers. De kans op een geslaagde phishing aanval is daardoor groter. De hacker krijgt bij een geslaagde aanval ook toegang tot de inhoud van de mailbox van deze medewerkers, die vaak gevoelige persoonsgegevens bevatten. Bijvoorbeeld gegevens van burgers die een hulpvraag hebben, zoals cliënten uit de Jeugdzorg en maatschappelijk ondersteuning. Geslaagde phishingaanvallen bij gemeenten kunnen de persoonlijke levenssfeer van burgers dan ook ernstig schaden. Daarnaast lopen burgers daardoor risico zelf ook slachtoffer te worden van phishing en/of spam berichten.

Voorbeeld datalekmelding: Phishing bij gemeente

Een gemeente doet een melding bij de AP over het volgende incident: Een medewerker van een gemeente heeft op een link in een phishing mail geklikt en vervolgens op een nep-pagina diens gebruikersnaam en wachtwoord ingevuld. Hiermee hebben onbevoegden toegang tot het mailaccount van de medewerker gekregen. De gemeente heeft onderzocht of er persoonsgegevens aanwezig waren in de mailbox van het getroffen account. Daaruit bleek dat de onbevoegden toegang hadden tot gegevens die door externen naar de gemeente zijn verstuurd. Daarbij ging het om persoonsgegevens van een groep cliënten uit de jeugdzorg en maatschappelijke ondersteuning. Deze cliënten zijn de volgende dag per brief geïnformeerd door de gemeente. Als maatregelen om de inbreuk aan te pakken heeft de gemeente direct het e-mailaccount geblokkeerd en de betrokken medewerker op de hoogte gebracht dat er sprake was van phishing. Daarnaast is de logging van alle overige mailadressen gecontroleerd op bijzondere activiteiten. Daarbij zijn geen afwijkingen geconstateerd. Als reactie op het incident is 2factor authenticatie (2FA) binnen de gemeente uitgerold. Het risico op succesvolle phishing-aanvallen wordt daarmee beperkt. Ook is de IT-beveiliging verder aangescherpt. Verdachte e-mails worden nu automatisch herkend door systeembeveiliging, die vervolgens een melding verstuurd aan de medewerker dat het mogelijk om een phishingmail gaat.

De AP constateert dat de gemeente het incident tijdig heeft gemeld, en onmiddellijk stappen heeft ondernomen om de schade van het datalek te beperken en nieuwe inbreuken te voorkomen. Daarnaast zijn de getroffen personen zonder vertraging, en op duidelijke wijze geïnformeerd over het datalek. De AP neemt daarom geen actie richting deze gemeente en sluit de melding af.

Datalekken bij gemeenten door te breed ingestelde autorisaties

Gemeenten ontvangen en versturen veel brieven met gevoelige persoonsgegevens. Bijvoorbeeld brieven in het kader van Jeugdzorg, Participatie, WMO, en gemeentelijke schuldhulpverlening. Veel gemeenten scannen al deze brieven in waarna ze worden opgeslagen in een gezamenlijk documentmanagementsysteem (DMS). Gevoelige HR-documenten van gemeente ambtenaren, zoals aanstellingsbrieven, gespreksverslagen van evaluatie- voortgangsgesprekken, en brieven omtrent re-integratietrajecten, worden ook vaak in het DMS opgeslagen.

Gemeenten moeten alle technische en organisatorische maatregelen treffen om ervoor te zorgen dat persoonsgegevens van burgers en medewerkers veilig zijn. Ingescande brieven en HR-documenten moeten daarom ook intern goed beveiligd worden. Wanneer dit niet goed is geregeld kan dat er onder meer toe leiden dat gemeentelijke ambtenaren in brieven kunnen kijken van burgers of collega's zonder dat dat noodzakelijk is voor de uitvoering van hun taken. Dit is een ernstige overtreding van de AVG. Onderzoeken door de AP naar dit soort overtredingen kunnen leiden tot sancties.

Voorbeeld datalekmelding: te breed ingestelde autorisaties bij gemeente

De AP ontving in 2019 een datalekmelding van een gemeente. In de melding is aangegeven dat vanwege het ontbreken van een autorisatiestructuur het documentmanagementsysteem (DMS) van de gemeente voor alle gebruikers (medewerkers) enige tijd open stond. Daarnaast was het gebruikersbestand onvoldoende actueel waardoor het voorkwam dat medewerkers nog rechten hadden op documenten van hun vorige werkplek. Dit had als gevolg dat veel gebruikers onbevoegd toegang hadden tot alle documenten in het DMS. Het DMS bevat onder meer alle inkomende post van de gemeente. Het datalek heeft betrekking op alle burgers, inwoners, leerlingen en medewerkers van de gemeente, een enorme groep mensen. Tussen de gegevens in de DMS zaten onder andere Burgerservicenummers, toegang- en identificatiegegevens, kopieën van paspoorten, gegevens over strafrechtelijke veroordelingen en gegevens over de gezondheid van burgers en medewerkers van de gemeente.

De AP neemt naar aanleiding van de melding contact op met de gemeente en de Functionaris Gegevensbescherming (FG) van de gemeente. De AP draagt de gemeente op om onmiddellijk de instellingen van de autorisatiestructuur aan te passen en beleid te implementeren om nieuwe inbreuken te voorkomen. Naar aanleiding van dit contact heeft de gemeente diverse maatregelen genomen waaronder het blokkeren van toegangsrechten tot het DMS, het toevoegen van beveiligingskenmerken van documentatie en het bestuderen van de logging. Uit nadere analyse van de logbestanden kon achteraf vastgesteld worden dat geen onrechtmatige raadpleging heeft plaatsgevonden.