AUTORITEIT
PERSOONSGEGEVENS

Meldplicht datalekken: facts & figures

Overzicht feiten en cijfers 2018

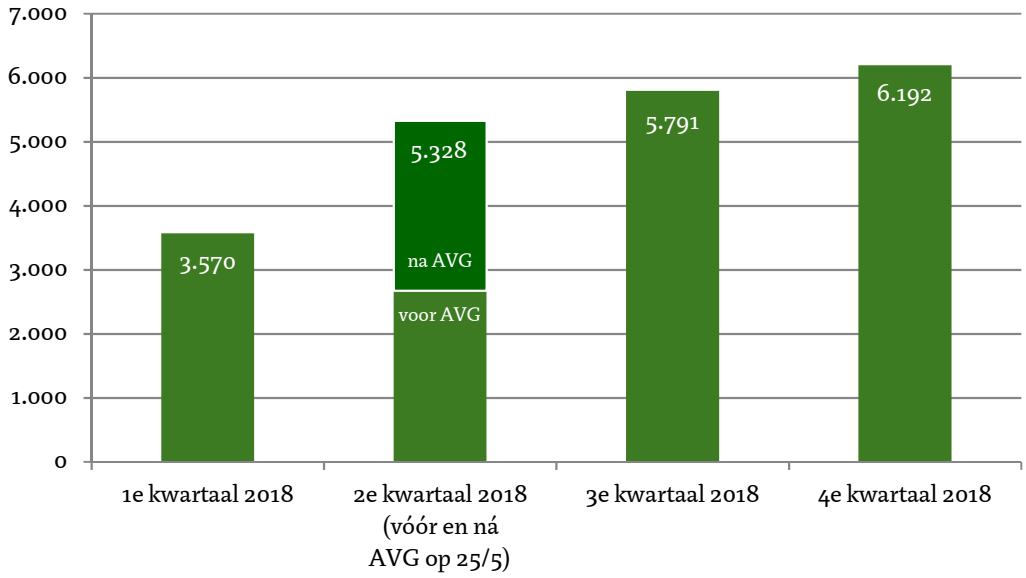
Aantal meldingen	Stijging	Type datalekken
20.881	↑ 109% ten opzichte van de 10.009 meldingen in 2017	63% persoonsgegevens verstuurd aan verkeerde ontvanger

Introductie

Organisaties moeten een datalek melden aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de personen waarvan de gegevens zijn gelekt. Organisaties moeten het datalek daarnaast melden aan de betrokken personen wanneer het lek kan leiden tot fysieke, materiële of immateriële schade voor deze betrokkenen. Het gaat dan om een situatie waarbij het lek waarschijnlijk een hoog risico voor de betrokkenen oplevert.

De meldplicht datalekken geldt in Nederland al sinds 2016. De meldplicht vloeit ook voort uit de Algemene verordening gegevensbescherming (AVG) die sinds 25 mei 2018 van toepassing is. Er zijn wel nuanceverschillen. Zo stelt de AVG strengere eisen aan de registratie van de datalekken in een organisatie. Organisaties moeten alle datalekken documenteren, inclusief de feiten over het datalek, de gevolgen daarvan en de genomen corrigerende maatregelen. Dat geldt ook voor datalekken die organisaties niet hoeven te melden. Met deze documentatie moet de AP kunnen controleren of organisaties aan de meldplicht datalekken hebben voldaan.

Aantal meldingen in 2018



In 2018 ontving de AP in totaal 20.881 meldingen van datalekken. Ten opzichte van voorgaande jaren is het aantal meldingen fors gestegen. In 2016 ontving de AP 5.849 meldingen van datalekken en in 2017 waren dat er 10.009. In 2018 is het aantal ten opzichte van 2017 dus ruim verdubbeld. Daarnaast hebben de andere Europese toezichthouders in 62 gevallen een grensoverschrijdend datalek gedeeld met de AP.

De invoering van de AVG op 25 mei 2018 vond plaats in het tweede kwartaal. Er is een sterke stijging van meldingen van datalekken zichtbaar in de laatste maand van dit kwartaal. Mogelijk komt dit door de gestegen(media-)aandacht voor de AVG.

Niet gemelde datalekken

De AP merkt dat niet alle meldplichtige datalekken door organisaties worden gemeld. Dat wordt bijvoorbeeld duidelijk als betrokkenen melding maken van een (meldplichtig) datalek, terwijl dat door de organisatie zelf niet is gemeld. De AP beschouwt dit als een ernstige zaak. Het totaal aantal datalekken dat gemeld had moeten worden in 2018 ligt dus nog hoger. In 2019 zal de AP zich meer focussen op deze niet gemelde datalekken. Onderzoeken die daaruit voortvloeien zullen mogelijk tot sancties leiden.

Belang van melden aan de AP en aan betrokkenen

Met de meldplicht aan de AP is beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. De AP moet door de verantwoordelijke worden geïnformeerd zodat de AP kan beoordelen of een onderzoek of het geven van aanwijzingen noodzakelijk is. 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.

Ondernomen acties door AP

Het efficiënt en effectief behandelen van datalekken staat centraal. In 2018 heeft de AP in veel gevallen uitleg gegeven aan organisaties over te nemen beveiligingsmaatregelen. Ook zijn brieven gestuurd om organisaties te wijzen op hun verantwoordelijkheid en zijn er normoverdragende gesprekken gevoerd.

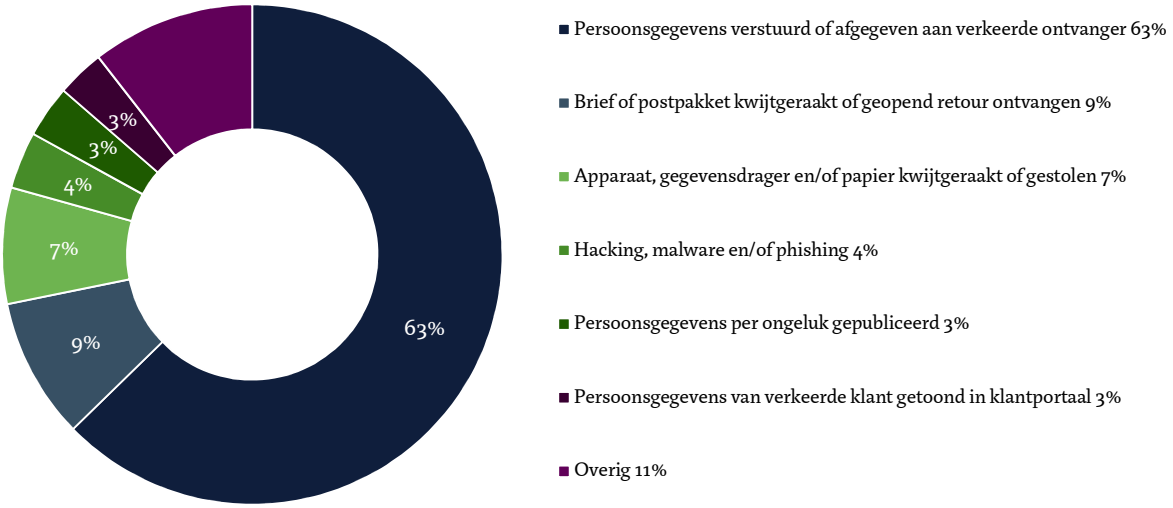
In 2018 heeft de AP 14.489 datalekmeldingen beoordeeld. Sinds 25 mei 2018 heeft de AP bij 298 datalekmeldingen actie ondernomen richting organisaties die een datalek gemeld hebben. Daarbij ging het om verschillende soorten acties. In 39% van de gevallen is contact opgenomen met de meldende organisatie om aanvullende informatie op te vragen over het datalek, in 35% van de gevallen is een normuitleggende brief gestuurd en in 23% van de gevallen is een normoverdragend gesprek gevoerd met de organisatie. In vier situaties is een onderzoek gestart naar aanleiding van de datalekmelding. Voor nog eens drie gevallen is initiatief genomen om een kortlopend onderzoek te starten.

Overtredingen van de meldplicht datalekken zullen in 2019 vaker leiden tot sancties. Daarom is groei in de capaciteit voorzien. In het bijzonder zal in 2019 aandacht worden geschonken aan het ten onrechte niet melden van datalekken aan betrokkenen of aan de AP en aan het te laat melden van een datalek. Ook beveiligingsproblemen, die de oorzaak waren van een datalek, kunnen aanleiding zijn voor een onderzoek.

Onderzoek naar datalek Uber

In november 2017 heeft Uber een groot datalek gemeld bij de AP. Dit datalek vond plaats in 2016 en is dus niet onverwijld gemeld aan de AP en aan betrokkenen. De AP heeft als leidende toezichthouder een internationale taskforce aangestuurd, bestaande uit privacytoezichthouders uit België, Duitsland, Frankrijk, Nederland, Italië, Spanje en het Verenigd Koninkrijk. De taskforce coördineerde de onderzoeken van de verschillende toezichthouders naar het betreffende datalek. De onderzoeken hebben uiteindelijk geleid tot het besluit van de AP om een bestuurlijke boete op te leggen aan Uber, ter hoogte van €600.000. De top van het Uber-concern was al eerder op de hoogte van het datalek, maar heeft niet tijdig gemeld aan de AP, noch aan de betrokkenen. De ernstig verwijtbare nalatigheid die Uber wordt aangerekend is van invloed geweest op de hoogte van deze in Nederland opgelegde boete.

Type datalekken



In de meerderheid van de gevallen betreft het datalek het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Hierbij gaat het met name om poststukken met gevoelige gegevens die bij de verkeerde persoon terechtkomen en geopend retour worden gestuurd (de onjuiste ontvanger heeft kennis genomen van de inhoud van de brief). Ook 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.

De meest gelekte gegevens zijn naam, geslacht en contactgegevens. Daarnaast zijn in 2018 ruim 6.000 meldingen ontvangen over gelekte medische gegevens (6.526) en het BSN (6.056). Een datalek met burgerservicenummers (BSN) komt met name voor in de zorg (37%) en in de sector openbaar bestuur (33%).

Datalekken door hacking en phishing komen met name voor in de zorg (18%). Bij phishing kan het gaan om organisaties die bestookt worden met nep e-mails die afkomstig lijken van een betrouwbare partij zoals een zakelijke relatie. Deze zijn soms nauwelijks van echt te onderscheiden. Wanneer een medewerker van de organisatie klikt op een link in de nep e-mail of een bijlage in de nep e-mail opent, kan daardoor een virus worden geïnstalleerd op het systeem dat persoonsgegevens treft. Een voorbeeld van zo'n virus is 'ransomware'. Dit is een type malware dat alle gegevens op het systeem versleuteld en ervoor zorgt dat deze gegevens niet meer toegankelijk zijn. Meestal wordt daarna betaling geëist, bijvoorbeeld via prepaidkaarten of Bitcoin.
Andere vormen van phishing zijn nep e-mails waarin een medewerker gevraagd wordt om het wachtwoord van zijn of haar account te wijzigen. De medewerker die op de link klikt wordt doorgeleid naar een nepwebsite waar de ingevoerde wachtwoordgegevens worden onderschept. Het onderschepte wachtwoord wordt vervolgens gebruikt om toegang te krijgen tot het account van de medewerker.

Waaronder toegang tot de inhoud van de mailbox. Accounts die op deze wijze worden gehackt, worden vaak misbruikt om nieuwe phishingmails te versturen.

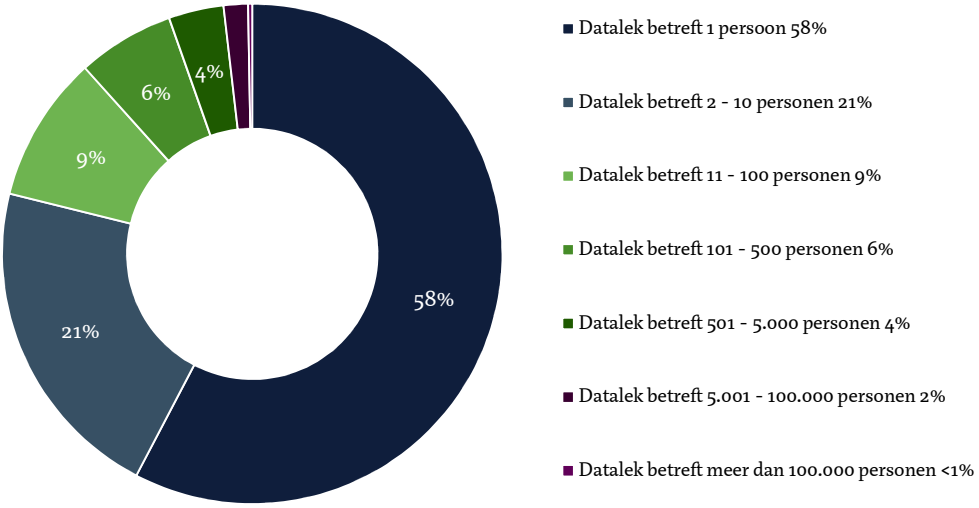
Phishingaanvallen die malware gebruiken, maken vaak misbruik van kwetsbaarheden in softwareprogramma's om de malware te installeren. Organisaties kunnen het risico op phishingaanvallen verkleinen door het installeren van antivirusprogramma's en spamfilters (firewalls) die kwaadaardige e-mails blokkeren en door deze regelmatig te updaten. Daarnaast is het belangrijk om medewerkers bewust te maken van phishing. Bijvoorbeeld door trainingen te organiseren met nagebootste phishingaanvallen.

Voorbeeld datalek: Phishing bij ziekenhuis

Een ziekenhuis meldt een datalek als gevolg van een phishingaanval. Een medewerker van het ziekenhuis heeft op een phishingmail geklikt en vervolgens zijn/haar inlognaam en wachtwoord ingevoerd. Hierdoor heeft een hacker toegang gekregen tot het account van de medewerker en heeft de hacker vanuit het account nieuwe phishingberichten verstuurd aan alle e-mailadressen in het adressenboek van het gehackte account. De geadresseerden zijn door de organisatie gewaarschuwd om de phishingmail niet te openen en direct te verwijderen.

De AP neemt naar aanleiding van de melding contact op en stelt aanvullende vragen. Onder andere of er mogelijk toegang is geweest tot de gegevens in de e-mailbox van de medewerker en welke maatregelen de organisatie neemt om phishing in de toekomst te voorkomen. Het ziekenhuis start vervolgens een onderzoek. Uit de resultaten van het onderzoek blijkt dat er medische gegevens van vijftien patiënten in de e-mailbox aanwezig waren en dat niet uitgesloten kan worden dat de hacker toegang heeft gekregen tot deze gegevens. Het ziekenhuis informeert de patiënten over het datalek. Ook organiseert het ziekenhuis trainingssessies om medewerkers bewust te maken van phishing en kwaadaardige e-mails te herkennen.

Aantal betrokkenen

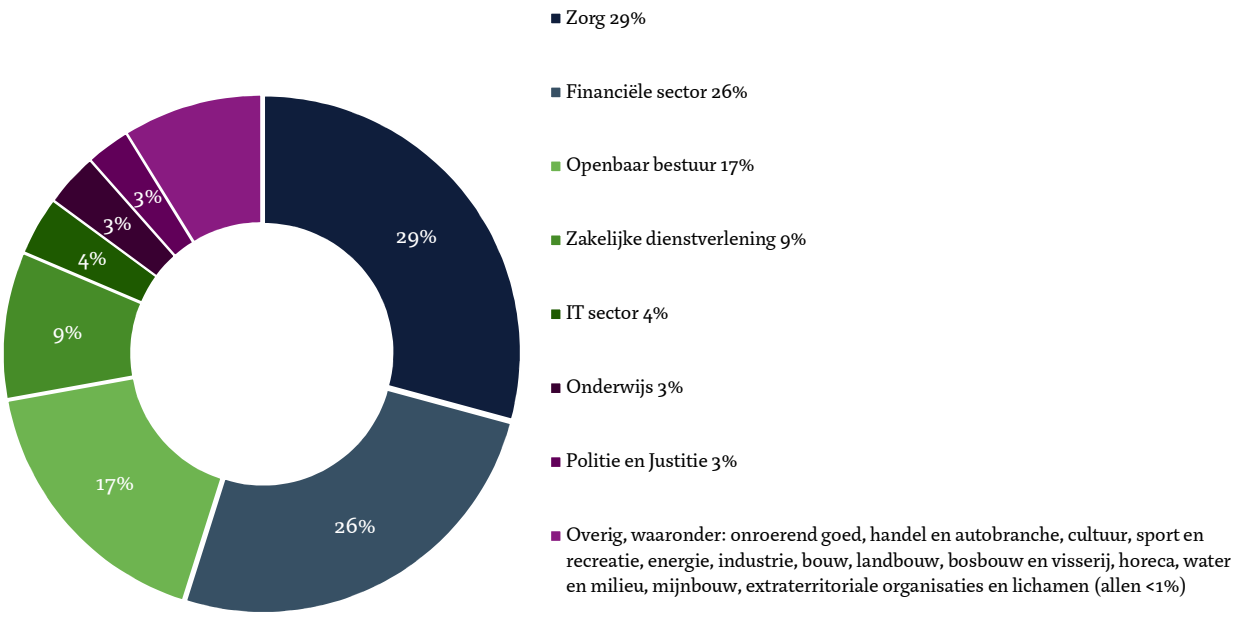


In de ruime meerderheid van de gevallen, namelijk 58%, raakt het datalek 1 persoon. Het gaat in deze gevallen veelal (77%) om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger.

In mindere mate (3%) treft het datalek een zeer groot aantal betrokkenen. Datalekken die 5.000 of meer personen raken, worden vaak veroorzaakt door hacking, malware en/of phishing.

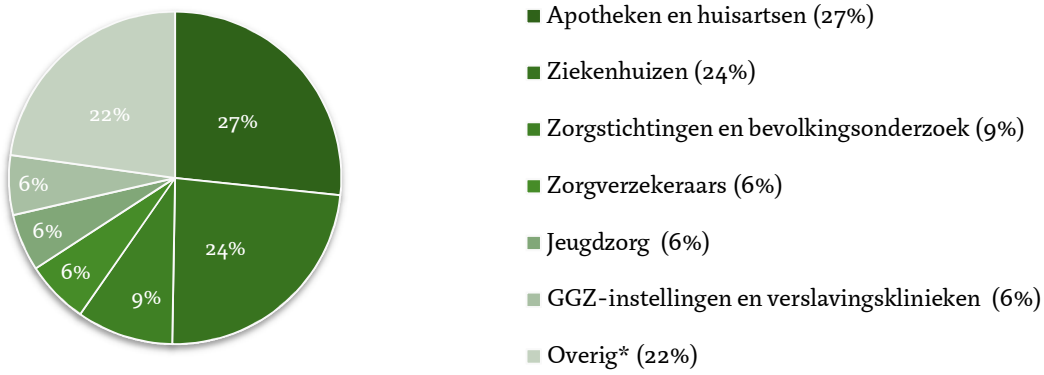
Voorbeeld datalek: Hacking met veel betrokkenen
Een organisatie doet een datalekmelding bij de AP waarin zij aangegeven dat de website van de organisatie is gehackt en er daarbij een 'skimmer' is geplaatst op het Content Management Systeem (CMS) van de website. Daardoor kunnen gegevens die bezoekers op de website invullen mogelijk worden onderschept. De organisatie geeft in de melding aan dat ze haar klanten niet informeert over het datalek omdat het volgens haar niet waarschijnlijk is dat betalingsgegevens van haar klanten zijn onderschept. De AP onderzoekt de website van de organisatie en stelt vast dat er via de website onder andere creditcardgegevens worden verwerkt. De AP stuurt een normoverdragende brief aan de organisatie. Naar aanleiding daarvan informeert de organisatie onmiddellijk alle 5.000 klanten die mogelijk zijn getroffen. De organisatie stelt de AP hiervan schriftelijk op de hoogte. Daarnaast kondigt de organisatie aanvullende beveiligingsmaatregelen aan om soortgelijke inbreuken in de toekomst te voorkomen.

Meldingen datalekken per sector



De meeste datalekken zijn gemeld vanuit de sector zorg (29%), de financiële sector (26%) en de sector openbaar bestuur (17%).

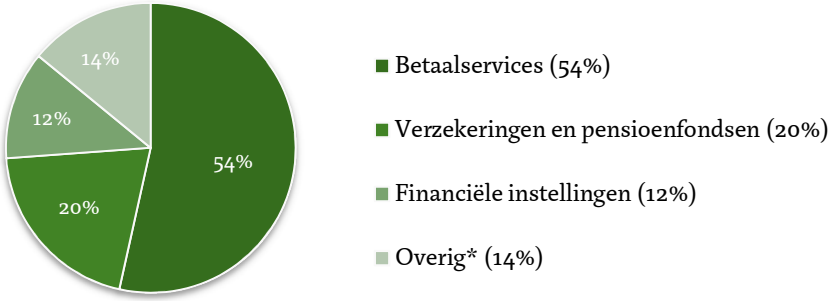
Zorg



* Onder 'overig' wordt o.a. verstaan: de maatschappelijke dienstverlening, verpleeghuizen, psychiaters, psychologen en fysiotherapeuten.

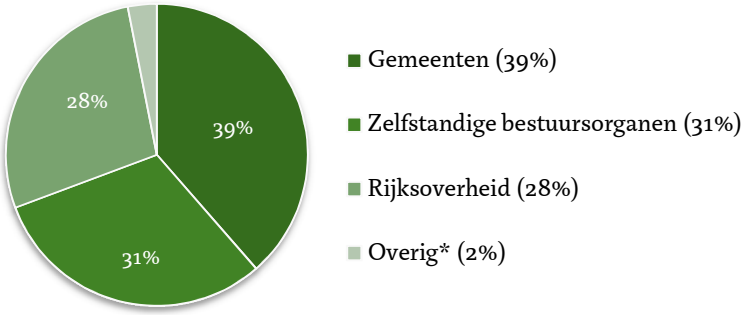
Voorbeeld datalek: diefstal persoonsgegevens uit auto
Een gemeente doet een melding van een datalek. Er is een tas van een medewerker van de afdeling Jeugdzorg uit diens auto gestolen. In de tas zat onder andere een laptop, een USB-stick en een mobiele telefoon met daarop gevoelige en bijzondere persoonsgegevens van jeugdigen die jeugdzorg krijgen en van hun ouders. De gegevens waren niet versleuteld opgeslagen. In de melding is aangegeven dat de betrokkenen op de hoogte zijn gebracht van het datalek. Verder heeft de organisatie aangegeven dat zij direct na ontdekking van de diefstal de wachtwoorden op de laptop en telefoon op afstand heeft gewist. De AP stuurt naar aanleiding van de melding een normoverdragende brief. In de brief wijst de AP de organisatie erop dat gevoelige gegevens op laptops, USB-sticks en telefoons passend dienen te worden beveiligd. Bijvoorbeeld door gebruik te maken van *encryptie* (versleuteling) en *remote wipe software* (wissen van gegevens op afstand). De organisatie dient deze norm toe te passen. Wanneer de AP na verzending van de brief constateert dat de organisatie haar gevoelige gegevens nog altijd niet adequaat beveiligt, kan de AP afhankelijk van de omstandigheden direct handhavend optreden tegen de organisatie.

Financiële sector



* Onder 'overig' bij financiële sector wordt o.a. verstaan financieel adviesbureaus en incassobureaus.

Openbaar bestuur



* Onder 'overig' bij openbaar bestuur wordt o.a. verstaan provincies, waterschappen en belastingen.