AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk
Ministerie van Financiën
Directoraat-Generaal Belastingdienst
Persoonsgegevens
Korte Voorhout 7
2511 CW DEN HAAG

Datum
10 december 2024

Ons kenmerk
2024-035022

Contactpersoon
Persoonsgegevens
070 8888 500

Onderwerp
Afhandelen datalekken

Geachte Persoonsgegevens

Inleiding
Op 26 september 2024 is door de Belastingdienst een presentatie verzorgd over het melden van datalekken aan medewerkers van de Autoriteit Persoonsgegevens (hierna: AP). Op 6 november 2024 heeft een nader overleg plaatsgevonden met medewerkers van de melddesk datalekken en medewerkers van het CPO-team, waaronder Persoonsgegevens van de Belastingdienst. Op 13 november 2024 zijn kopieën van het werkproces van de melddesk datalekken van de Belastingdienst met de AP gedeeld. Ook de procedure voor het behandelen van datalekken is toegezonden.

Conclusie en doel van deze brief
De AP constateert dat door de Belastingdienst veel energie is gestoken in de ontwikkeling van een organisatiebreed beleid voor de naleving van de meldplicht datalekken uit de Algemene Verordening Gegevensbescherming (AVG) en de Wpg (Wet Politiegegevens), en een zorgvuldige uitvoering daarvan. Er is dan ook aantoonbaar progressie geboekt om de naleving van de meldplicht uit de AVG en Wpg in lijn te brengen met de wettelijke uitgangspunten. Het proces behoeft op enkele punten nog verbetering. De verbeterpunten zijn in deze brief opgenomen en geformuleerd in de vorm van aanbevelingen. Bij het formuleren van de aanbevelingen volgen we de fases van het werkproces.

Ontvangst incidenten en meldingen, toepassing registratiesysteem
Signalen over beveiligingsincidenten, en dus ook mogelijke datalekken, worden gemeld via de e-mail, de Belastingtelefoon of een inbox. Incidenteel kan een signaal ook door de Functionaris voor de Gegevensbescherming (FG) worden ontvangen.

Het gebruikte registratiesysteem voor beveiligingsincidenten, bestaande uit gemelde datalekken en niet-gemelde datalekken, geldt ook als wettelijk verplichte interne incidentenregistratie. Per april 2023 wordt daarvoor gebruik gemaakt van één nieuwe applicatie. Voorheen waren hier circa vier applicaties voor nodig die voor een totaaloverzicht eerst gecombineerd moesten worden. De door de melder opgegeven informatie wordt door de behandelaar van de melddesk datalekken in het registratieformulier nader aangevuld. De behandelaar van de melddesk datalekken beoordeelt en beslist of het gemelde beveiligingsincident ook moet worden gekwalificeerd als een datalek in de zin van de AVG en/of de Wpg. Om eventuele navraag te kunnen doen bij de melder bleek dat in het registratieformulier in het systeem ook het BSN van de melder wordt geregistreerd. Binnen het systeem kan gefilterd worden op alle criteria uit het registratieformulier. Het systeem genereert vervolgens per individuele registratie een wegingsformulier.

> **Aanbeveling 1**
> Het vastleggen van het BSN van de melder voor het bovenbeschreven doel is waarschijnlijk niet toegestaan. Wij verzoeken u na te gaan in welke situaties het BSN wordt geregistreerd en of deze verwerking noodzakelijk is in het kader van de uitvoering van de publieke taak van de Belastingdienst.[1]

Controle en overleg

Na controle (vierogen-principe) door een collega en eventuele aanpassingen wordt het wegingsformulier gezonden naar de contactpersoon en directeur binnen een directie. Bij interne verschillen van inzicht wordt de coördinerend specialistisch adviseur privacy en gegevensbescherming van het CPO-team van de belastingdienst geraadpleegd. Daarnaast is er een wekelijks overleg tussen betrokken medewerkers waarin ruimte is om te spreken over individuele lastig te maken risico-afwegingen. Op informele basis is er contact met de FG.

Rapportage

Vanuit de bronbestanden worden de geregistreerde inbreuken maandelijks gerapporteerd aan alle directeuren en aan alle datacoördinatoren binnen de Belastingdienst.[2] Eens per vier maanden wordt ook een uitgebreidere rapportage uitgebracht aan alle directeuren en datacoördinatoren binnen de Belastingdienst. Na een bewaartermijn van drie jaren worden de gerapporteerde incidenten opgeschoond in het registratiesysteem. De toepassing van die termijn wordt nu ook gecontroleerd bij de registraties in Excelformulieren, die nog dateren uit de periode voordat het huidige systeem in gebruik werd genomen. Bezien wordt of die informatie begin 2025 verwijderd en vernietigd kan worden.

Volledigheid overzicht ontvangen meldingen

Het aantal meldingen van een datalek dat de Belastingdienst doet aan de AP is, gelet op de omvang van de organisatie en het type dienstverlening, relatief laag in vergelijking met soortgelijke overheidsorganisaties. Hoewel de AP het standpunt van de Belastingdienst deelt dat het niet eenduidig te benoemen is welke meldingen mogelijk misgelopen worden, denkt de AP dat er een gerede kans is dat bepaalde datalekken

[1] Zie artikel 10 van de Wet algemene bepalingen burgerservicenummer (Wabb).
[2] De melddesk datalekken werkt overigens ook voor de Douane en Toeslagen.

0001

momenteel door de Belastingdienst gemist worden. Uit alle verkregen informatie volgt bijvoorbeeld dat de melddesk datalekken van de Belastingdienst beleid hanteert waarin onderscheid wordt gemaakt tussen damages (fouten in systeem) en datalekken. De AP wijst er op dat 'een tijdelijke onbeschikbaarheid' van persoonsgegevens ook een mogelijk meldplichtig datalek kan zijn. Hoewel 'damages' wel vermeld worden op de website van de Belastingdienst en worden opgenomen in de incidentenregistratie, dient per individueel geval nagegaan te worden of dit niet ook een datalek is, en zo ja, of dit datalek gemeld moet worden aan de AP en aan de betrokkenen.

Aanbeveling 2
De AP adviseert om in de bewustwordingstrainingen voor nieuwe én voor zittende medewerkers voldoende aandacht te schenken aan het herkennen van inbreuken op de integriteit, vertrouwelijkheid én beschikbaarheid van persoonsgegevens, en het melden van dergelijke inbreuken bij de melddesk datalekken.

Aanbeveling 3
Om te controleren of het intern datalekregister volledig is, vragen wij u om te onderzoeken of (tijdelijke) inbreuken op de beschikbaarheid van persoonsgegevens ook zijn opgenomen in het datalekregister. De AP adviseert tevens om na te gaan bij de IT-afdeling, het Security Operations Center (SOC) en/of een andere toepasselijke eenheid binnen de Belastingdienst, of er in de tweede helft van 2024 'damages' zijn geregistreerd die ook aangemerkt kunnen worden als een (tijdelijke) inbreuk op de beschikbaarheid, en zo ja: of deze zijn opgenomen in het datalekregister en of deze gemeld hadden moeten worden aan de AP en aan de betrokkenen.

Aanbeveling 4
De AP beveelt aan om de FG van de Belastingdienst volgens een vaste en gedocumenteerde werkwijze te betrekken bij de afhandeling van datalekken die binnen organisatie plaatsvinden, met name wanneer er twijfel of onduidelijkheid bestaat over de ernst van de gevolgen van het datalek voor de betrokkenen.[3] De AP beveelt aan om nauwkeuriger in het beleid vast te leggen wanneer de FG betrokken moet worden. In het datalekken-registratiesysteem kan voorts een extra opmerkingenveld worden toegevoegd waarin de FG optioneel zijn/haar advies kan geven, zodat ook goed beoordeeld kan worden of bij de afwikkeling van een melding afgeweken is van het advies van de FG.

Informeren van betrokkenen
Indien uit de risico-afweging volgt dat een incident als datalek gemeld moet worden aan de AP en aan de betrokkenen, dan informeert de medewerker van de melddesk datalekken de directeur van het dienstonderdeel waarbinnen het incident heeft plaatsgevonden. Tijdens het gesprek is aangegeven dat de

[3] Zie ook de Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, WP250rev.01, pagina 32. Hierin is opgenomen dat de FG een sleutelrol dient te spelen bij de preventie van datalekken door advies te verstrekken en door toe te zien op de naleving van de meldplicht datalekken. Het wordt aanbevolen om de FG onmiddellijk op de hoogte te brengen van het bestaan van een datalek, en de FG te betrekken bij het gehele proces om het datalek te beheren en te melden.

0001

voortvarendheid waarmee het informeren van betrokkenen geschiedt nu nog veel per directie verschilt. Om te voorkomen dat het informeren van betrokkenen onnodig lang op zich laat wachten ontvangt de directeur van het desbetreffende dienstonderdeel herhaaldelijk een periodieke melding van de melddesk datalekken, totdat is bevestigd dat de betrokkenen zijn geïnformeerd. De directeur van het bij het datalek betrokken dienstonderdeel beslist uiteindelijk over de praktische uitvoering om het incident te melden aan de betrokkenen. Indien een directeur naar eigen inzicht besluit af te zien van het informeren van betrokkenen, tegen het advies van de melddesk datalekken in, dan dient de directeur dit te motiveren. Deze motivatie wordt in voorkomende gevallen in het dossier in het registratiesysteem opgenomen. Door de medewerkers van de Belastingdienst is aangegeven dat het slechts sporadisch voorkomt dat de directeur afwijkt van het advies van de melddesk datalekken.

Aanbeveling 5
De AP beveelt aan om in gevallen waarbij de directeur afwijkt van het advies van de melddesk datalekken, of voornemens is om af te wijken van dit advies, altijd de FG te betrekken, en het advies van de FG toe te voegen aan het dossier in het registratiesysteem. De AP beveelt voorts aan om jaarlijks aan de DG te rapporteren hoe vaak door het management wordt afgeweken van het advies van de melddesk datalekken om betrokkenen te informeren, en wat de reden daarvoor was.

Melding aan de AP in geval van encrypted devices

Tijdens het gesprek kwam aan bod dat vermiste, maar encrypted devices (smartphones, tablets, etc.) tot op heden door de Belastingdienst als een datalek worden gemeld bij de AP. De AP bevestigt via deze brief dat de Belastingdienst geen datalekken (meer) bij de AP hoeft te melden als het gaat om vermiste mobiele devices die goed beveiligd zijn door de toepassing van encryptie, mits de Belastingdienst beschikt over actuele kopieën of back-ups van de persoonsgegevens die op de vermiste mobiele device stonden. Deze incidenten dienen overigens wel intern geregistreerd te worden in het datalekregister van de Belastingdienst.

Monitoring

Medio 2025 zal de AP nagaan of de aanbevelingen toereikend zijn opgevolgd.

Tot slot

Een afschrift van deze brief zal worden gestuurd aan Persoonsgegevens het Ministerie van Financiën.

Datum
10 december 2024

Ons kenmerk
2024-035022

De AP hoopt u hiermee voldoende te hebben geïnformeerd. Indien u vragen heeft over deze brief kunt u contact opnemen met bovengenoemde contactpersoon.

Hoogachtend,
Autoriteit Persoonsgegevens,
Namens deze,

Persoonsgegevens

Programmadirecteur

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

Ministerie van Financiën
Staatssecretaris van Financiën – Fiscaliteit en Belastingdienst
De heer drs. T. van Oostenbruggen
Postbus 20201
2500 EE DEN HAAG

Datum
23 december 2024

Ons kenmerk
2024-035019

Contactpersoon
Persoonsgegevens

Onderwerp
Opdracht ter verbetering van de privacyorganisatie van de Belastingdienst

Geachte heer Van Oostenbruggen,

In april 2024 heeft de Autoriteit Persoonsgegevens (AP) een toezichtarrangement ingesteld met als doel het realiseren van een duurzame verbetering van de bescherming van persoonsgegevens door de Belastingdienst.[1] Een van de aangekondigde thema's van het toezicht betreft de privacyorganisatie van de Belastingdienst. De privacyorganisatie vervult immers, tezamen met de Functionaris voor Gegevensbescherming (FG), een cruciale rol bij het realiseren van een cyclus van continue verbetering op het punt van de bescherming van persoonsgegevens. De AP heeft om die reden de afgelopen maanden de huidige staat van de privacyorganisatie onderzocht, waarbij mede is gekeken naar de ontwikkelingen die hebben plaatsgevonden sinds de brieven van de AP uit 2021 en 2022.[2] U ontvangt hierbij de conclusies van dit onderzoek. Centraal in het onderzoek stond de governance van de privacyorganisatie.

Conclusie

De AP concludeert dat er sinds haar adviezen uit 2021 en 2022 positieve ontwikkelingen zichtbaar zijn in de staat van de privacyorganisatie, maar dat er op een aantal punten dringend aandacht nodig is om de privacyorganisatie naar behoren te laten functioneren. De AP heeft met name serieuze zorgen over onduidelijkheden rondom het beleggen van verantwoordelijkheden en de invulling van taken, en de gebrekkige centrale regie. De AP roept u daarom op om de governance van de privacyorganisatie te herijken en te versterken. De AP vindt het voorts van groot belang de formatie van het FG-team minimaal op 6 fte te houden.

[1] Brief van 19 april 2024 met kenmerk 2024-28-AWO-GBU.
[2] Brief van 27 oktober 2021 met kenmerk z2020-01800 en brief van 30 augustus 2022 met kenmerk z2022-03882. Beide brieven zijn gericht aan de Staatssecretaris van Financiën – Fiscaliteit en Belastingdienst.

0001

Eerdere adviezen van de AP aangaande de privacyorganisatie en de positie van de FG

In de brief van 27 oktober 2021 merkte de AP op dat de privacyorganisatie van de Belastingdienst op dat moment nog onvoldoende solide was om haar functie naar behoren te kunnen vervullen. Aangeraden werd om een gelaagde structuur aan te leggen van medewerkers met voldoende kennis en ervaring met privacy, wat resulteert in één aanspreekpunt (de Chief Privacy Officer). Ook werd aangeraden om de (verwerkings)verantwoordelijkheden binnen de Belastingdienst en het Ministerie van Financiën helder vast te leggen. In de brief werd tevens verzocht om na te gaan of de FG over voldoende middelen beschikt, zeker nu het FG-team werkt voor het gehele Ministerie van Financiën. Geconstateerd werd dat de toenmalige versterking had geleid tot drie additionele functies. De AP vroeg zich af of deze uitbreiding voldoende was om de naleving binnen uw organisatie op orde te krijgen.
In de brief van de AP van 30 augustus 2022, waarmee de AP haar advies gaf op het departementale actieplan Privacy op Orde, werd aangegeven dat de specifieke inhoudelijke inrichting van het actieplan voor de Belastingdienst te weinig concreet en te beperkt in ambitie was om de zorgen van de AP weg te nemen.

Positieve ontwikkelingen

De AP ziet dat de Belastingdienst sinds de eerdere adviezen veel medewerkers heeft aangenomen met specialistische kennis over de Algemene Verordening Gegevensbescherming (AVG). Zo is er een vaktechnische structuur ingericht, bestaande uit circa 70 medewerkers, waardoor meer specialistische AVG kennis op de werkvloer aanwezig is. Belastinginspecteurs hebben hierdoor de mogelijkheid om bij AVG vragen snel te schakelen met deze specialisten. De medewerkers binnen de vaktechnische structuur dragen bovendien bij aan de bewustwording ten aanzien van de zorgvuldige omgang met persoonsgegevens, onder meer door het geven van presentaties. Daarnaast werken er nu zo'n 20 datacoördinatoren bij de verschillende directies. Deze medewerkers zijn vooral betrokken bij privacymanagementvraagstukken, zoals het opstellen van DPIA's. Deze zomer is een Chief Privacy Officer (CPO) aangesteld die zich volledig kan richten op deze functie. Ook is het CPO-team, dat is ondergebracht bij de kaderstellende directie Informatievoorziening en databeheersing (IV&D), versterkt. Voorts is de basis gelegd voor het inrichten van vaste overlegmomenten tussen de vaktechnische structuur, het CPO-team en de andere actoren binnen de privacyorganisatie. Tot slot constateert de AP dat er verschillende programma's lopen, of al zijn afgerond, die de naleving van de AVG binnen de Belastingdienst ondersteunen en verbeteren.[3]

Noodzakelijke verbeteringen

De AP constateert dat verbeteringen noodzakelijk zijn op het punt van:

1. het creëren van duidelijkheid rondom taken en verantwoordelijkheden, en de governance van de privacyorganisatie;
2. de centrale regie op het geheel, waaronder het opstellen van richtinggevende kaders.

De AP komt tot deze conclusie na het bestuderen van documenten en het voeren van gesprekken met functionarissen binnen de privacyorganisatie.[4]

[3] Een voorbeeld hiervan is het programma Fiscale Meldingen & Informatiestromen.
[4] Er is gesproken met medewerkers van IV&D, de Corporate Dienst Vaktechniek en van vier doelgroepdirecties.

0001

1. Taken/verantwoordelijkheden zijn niet duidelijk en liggen niet vast

De AP concludeert dat er weliswaar veel mensen zijn aangenomen, maar dat er onvoldoende samenhang bestaat tussen de verschillende functionarissen. Er bestaat onduidelijkheid over elkaars taken en rollen. Er is geen overzicht van de verschillende rollen en verantwoordelijkheden binnen de privacyorganisatie. Diverse functionarissen werken aan privacy gerelateerde vraagstukken:

- de circa 70 medewerkers binnen de vaktechnische lijn (Corporate Dienst Vaktechniek, VT);
- de circa 20 datacoördinatoren (werkzaam binnen de verschillende doelgroepdirecties);
- de circa 7 medewerkers van het CPO-team.

Ook medewerkers van de concerndirectie Fiscaal Juridische Zaken (FJZ), van de directie Bestuurlijke en Politieke Zaken (BPZ) en de Concerndirectie Uitvoerings- en Handhavingsbeleid (UHB) worden geraadpleegd bij privacy gerelateerde vraagstukken. Geregeld is echter niet duidelijk wie om welke reden bij een vraagstuk betrokken wordt, of moet worden.

Binnen de directie IV&D bestaat een afdeling met de naam Achitectuur en Dataoffice. Binnen deze afdeling zijn twee teams ondergebracht: het team met architecten en de CDO-office. De Belastingdienst kent een sterke architectuursturing. De architecten modelleren nieuwe bedrijfsprocessen en bepalen of de noodzakelijke IT zelf wordt ontwikkeld, of wordt ingekocht. Het is daarbij van belang om tijdig na te gaan of de noodzakelijke DPIA's zijn uitgevoerd. Het CDO-office maakt kaders en beleid op het gebied van datamanagement. Bij de totstandkoming van die kaders wordt nog onvoldoende afgestemd met het CPO-team.

Daarnaast lopen er binnen de Belastingdienst diverse programma's en projecten ter verbetering van de naleving van de AVG. Ook vanuit die programma's en projecten wordt geregeld onvoldoende contact gelegd met het CPO-team. Als datacoördinatoren worden betrokken gebeurt dat vaak ad hoc.

Uit het gesprek dat de AP met een aantal datacoördinatoren voerde bleek dat de rol van datacoördinator per directie verschilt, en dat de invulling mede afhankelijk is van de vraag hoe de directie die invulling wil regelen. De functiebenamingen zijn ook niet eenduidig. Nergens ligt vast bij welke vraagstukken de datacoördinatoren betrokken moeten worden. Er is discussie over de vraag wie de opleiding voor de datacoördinatoren moet regelen: de dienst VT of de directie IV&D. De datacoördinatoren benadrukken dat de verantwoordelijkheden binnen de organisatie niet goed zijn belegd en dat niet duidelijk is wat ieders rol is binnen de privacyorganisatie. De datacoördinatoren vervullen een rol bij het opstellen van DPIA's, maar vaak is onduidelijk wie binnen de Belastingdienst de (verwerkings)verantwoordelijke is voor het proces. Dat hangt vooral samen met de structuur van de Belastingdienst met directies en ketens.

De AP constateert dat er sprake is van versnippering. Er is onvoldoende beschreven welk team welke taak uitvoert binnen de privacyorganisatie. Ook is onduidelijk wie eventuele risico's accepteert, of maatregelen moet treffen om de risico's te mitigeren. De governance is niet duidelijk geregeld. Hierdoor wordt er geregeld langs elkaar heen gewerkt en wordt er soms ook onnodig op elkaar gewacht. Deze situatie maakt het mogelijk dat verantwoordelijkheden worden afgeschoven of dat onderwerpen juist worden opgepakt

terwijl men er niet over zou (moeten) gaan. De onduidelijkheid veroorzaakt ook shopgedrag, waarbij meerdere actoren worden geraadpleegd teneinde een gewenst antwoord te krijgen.

De AP constateert dat er nog geen zichtbare stappen zijn gezet om taken en verantwoordelijkheden beter te definiëren.

2. Ontoereikende centrale regie, beperkte invulling kaderstellende rol

In het verlengde van het vorige punt constateert de AP dat er geen totaalbeeld bestaat van de activiteiten die momenteel worden verricht binnen de organisatie om de naleving van de AVG te verbeteren. Ook is er geen inzicht in de activiteiten die nog moeten worden verricht om dat doel te bereiken. De centrale coördinatie is onvoldoende. Er is binnen de privacyorganisatie sprake van gefragmenteerde sturing, en onvoldoende samenwerking. De structuur van de Belastingdienst met vele directies en ketens maakt het inrichten van centrale regie overigens extra complex, terwijl juist binnen deze structuur sterke regie essentieel is.

De directie IV&D is een kaderstellende directie. Er zijn echter nauwelijks kaders opgesteld op het gebied van privacymanagement en privacy inhoudelijke vraagstukken die medewerkers van de Belastingdienst kunnen gebruiken in hun werk. Er zijn kaders voor het melden van datalekken en het afhandelen van inzageverzoeken. Deze kaders zijn echter niet goed vindbaar, of niet breed bekend. Er bestaat op dit moment ook verschil van inzicht in de vraag vanuit welke directie kaderstellende documenten moeten worden opgesteld die betrekking hebben op privacy inhoudelijke vraagstukken.

Zonder heldere kaders is het moeilijk om vanuit een kaderstellende directie, zoals IV&D, invulling te geven aan het uitvoeren van controles om na te gaan of de directies in het primaire proces hun verantwoordelijkheden daadwerkelijk nemen, en de AVG en de Wpg (Wet Politiegegevens) naleven. Dergelijke controles vinden vanuit het CPO-team nog nauwelijks plaats.

Intern toezicht FG

Aan het FG-team was tot voor kort een formatie toegekend van 6 fte. Het kent op dit moment een formatie van 5 fte. Omdat dit team voor het gehele Ministerie van Financiën opereert is de destijds toegekende formatie van 6 fte naar de overtuiging van de AP minimaal nodig om de wettelijke taken goed uit te kunnen voeren. Dat geldt temeer nu er bij in elk geval de Belastingdienst nog de nodige stappen gezet moeten worden om de naleving van de AVG verder te versterken. De AP beschouwt de eerder toegekende bezetting voor de FG dan ook als minimaal en roept u in verband daarmee op om zorg te dragen voor in ieder geval deze minimale bezetting.

Opdracht

De AP verzoekt u de governance van de privacyorganisatie te herijken en te versterken. Onderdeel daarvan is het verduidelijken van de taken en verantwoordelijkheden van de verschillende functies binnen de privacyorganisatie, en het concreet beschrijven daarvan. Daarbij moet worden gelet op de onderlinge samenhang tussen de functies. Ook de besluitvormings- en de overlegstructuur moeten versterkt worden. Voor elke medewerker van de Belastingdienst moet duidelijk zijn voor welke vraag hij/zij bij welke

0001

functionaris moet zijn. Ook moet duidelijk zijn wie eventuele risico's moet accepteren, of maatregelen moet treffen om de risico's te mitigeren.

Met het oog op de bescherming van de belangen van de burgers moet worden nagegaan of de organisatie in staat is om de verantwoordelijkheden die uit de AVG voortvloeien in voldoende mate op te pakken, en welke onderdelen extra aandacht behoeven.

Gelet op de structuur van de Belastingdienst met een combinatie van lijn- en ketensturing is het van belang om helder te maken welke lijn of keten primair verantwoordelijk is als het gaat om gespecificeerde privacyvraagstukken.

De centrale regie moet versterkt worden. De directie IV&D, en het CPO-team in het bijzonder, spelen hierbij een belangrijke rol.

De nieuwe governance kan worden vastgelegd in een specifiek privacybeleid voor de Belastingdienst.

Tot slot

Het is essentieel de governance zo in te richten dat dit bijdraagt aan processen en systemen die voorkomen dat onterechte negatieve effecten optreden voor burgers. Een goed werkende privacystructuur kan bijvoorbeeld de kans op discriminatoir handelen minimaliseren. Dit zal bijdragen aan het herstel van het vertrouwen van de burger in de Belastingdienst. Een goed werkende privacystructuur zal voorts het werkplezier van medewerkers die werkzaam zijn binnen die structuur doen vergroten.

De AP zal in het najaar van 2025 nagaan of de noodzakelijke verbeteringen zijn doorgevoerd.

De AP zendt een afschrift van deze brief aan uw Functionaris voor Gegevensbescherming. Deze brief wordt op 13 januari 2025 op de website van de AP gepubliceerd.

Hoogachtend,
Autoriteit Persoonsgegevens

Persoonsgegevens

Bestuurslid

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

Ministerie van Financiën
Directoraat-Generaal Belastingdienst
Persoonsgegevens
Korte Voorhout 7
2511 CW Den Haag

Datum
28 januari 2025

Ons kenmerk
2025-000652

Contactpersoon
Persoonsgegevens

Onderwerp
Ontheffing fiscale geheimhoudingsplicht in gevallen van vermoedelijke fiscale integriteitsschending op grond van artikel 67, derde lid van de Awr

Geachte Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) heeft op 1 februari 2024 een normoverdragend gesprek gevoerd over de ontheffing van de fiscale geheimhouding in het kader van het integriteitsbeleid. De ontheffing vindt plaats op grond van artikel 67, derde lid van de Awr. De AP verzocht de Belastingdienst om met de verwerking te stoppen en het beleid en de werkwijze te heroverwegen. De Belastingdienst heeft de verwerking vervolgens opgeschort. In het gesprek op 10 december 2024 zijn conclusies geformuleerd voor het vervolg.

Conclusie

Artikel 67, derde lid van de Awr is geformuleerd als een vrijwel ongeclausuleerde uitzonderingsbepaling. De AP heeft daarover haar zorgen uitgesproken, gezien de grote impact die de ontheffing kan hebben op betrokkenen. De AP is van mening dat de vrijwel ongeclausuleerde ontheffingsgrond uit artikel 67, derde lid van de Awr om fiscale gegevens te verwerken en/of te delen in het kader van een integriteitsonderzoek op zichzelf weinig precies en voorzienbaar is voor betrokkenen. De AP verzoekt de Belastingdienst te onderzoeken op welke wijze artikel 67, derde lid van de Awr kan worden aangepast.
De AP onderkent dat het aanpassen van de bepaling tijd kost. De AP concludeert dat indien de Belastingdienst een beleidsregel maakt voor de toepassing van artikel 67, derde lid van de Awr voor gevallen van vermoedelijke fiscale integriteitsschendingen, waarin voldoende aanvullende waarborgen worden opgenomen ten behoeve van het recht op gegevensbescherming van betrokkenen, de Belastingdienst weer kan beginnen met deze verwerking. Dit vooruitlopend op de wetswijziging. Voorbeelden van zulke aanvullende waarborgen worden beschreven in deze brief.

Datum
28 januari 2025

Ons kenmerk
2025-000652

Aanleiding

De AP heeft op 1 februari 2024 een normoverdragend gesprek gevoerd met de Belastingdienst. In dit gesprek heeft de AP haar zorgen geuit over de ontheffing van de fiscale geheimhoudingsplicht op grond van artikel 67, derde lid van de Awr in zaken van vermoedelijke fiscale integriteitsschendingen door medewerkers van de Belastingdienst.
Wanneer er sprake is van een ernstig vermoeden van fiscale integriteitsschending door een medewerker van het Ministerie van Financiën, kan de inspecteur de staatssecretaris van Financiën verzoeken om een ontheffing van zijn fiscale geheimhoudingsplicht als bedoeld in artikel 67, derde lid van de Awr om fiscale gegevens te delen opdat de werkgever onderzoek kan doen of sprake is van een integriteitsschending en of er arbeidsrechtelijk moet worden opgetreden. In het geval van twee AVG-klachten, ingediend bij de AP en die de aanleiding waren voor de AP om in gesprek te gaan met de Belastingdienst, heeft de inspecteur van de Belastingdienst de uitzonderingsgrond uit artikel 67, derde lid van de Awr gebruikt om fiscale gegevens over deze belastingplichtigen (tevens werknemers) te delen met de Belastingdienst (Staat der Nederlanden, vertegenwoordigd door de minister van Financiën) als zijnde werkgever. Na het normoverdragende gesprek van 1 februari 2024 heeft de Belastingdienst, op verzoek van de AP, de verwerking gestopt. De AP heeft voorts gevraagd het beleid en de werkwijze te heroverwegen. De Belastingdienst heeft in een brief van 14 juli 2024 gevraagd om een vervolggesprek.

Zorgen van de AP over artikel 67, derde lid van de Awr

In het vervolggesprek van 10 december 2024, heeft de AP nogmaals haar zorgen geuit over artikel 67, derde lid van de Awr. Artikel 67, derde lid van de Awr is geformuleerd als een vrijwel ongeclausuleerde uitzonderingsbepaling. De AP vindt dit zorgelijk, gezien de grote impact die de ontheffing kan hebben op betrokkenen. De AP is van mening dat de vrijwel ongeclausuleerde ontheffingsgrond uit artikel 67, derde lid van de Awr op zichzelf weinig precies en voorzienbaar is voor betrokkenen. Daarnaast vindt de AP het zorgelijk dat de formulering van artikel 67, derde lid van de Awr de Belastingdienst de mogelijkheid lijkt te bieden om regulier een beroep te doen op deze ontheffingsgrond als zijnde een soort restcategorie.
Deze praktijk zou mogelijk kunnen leiden tot een uitholling van het enge ontheffingsstelsel dat de wetgever beoogd heeft. De AP verzoekt de Belastingdienst te onderzoeken op welke wijze artikel 67, derde lid van de Awr kan worden aangepast.

Het vaststellen van een ministeriële regeling op grond van artikel 67, tweede lid, onderdeel b van de Awr is voor dit type verstrekkingen niet voor de hand liggend, alleen al omdat het in casu niet gaat om verstrekkingen aan een bestuursorgaan.

Beleidsregel met aanvullende waarborgen

Aanpassing van artikel 67, derde lid van de Awr, zal enige tijd vergen. In de tussentijd steunt de AP het opstellen van een beleidsregel waarin voldoende waarborgen zijn opgenomen voor de bescherming van de persoonsgegevens van de burger. Het doel van deze beleidsregel is om het verwerkingsproces van een verzoek opheffing geheimhouding voorzienbaarder en transparanter te maken.
Door de Belastingdienst is reeds een Commissie advisering ontheffing geheimhoudingsplicht ingesteld. Deze commissie adviseert de staatssecretaris, via de hoofddirecteur Fiscale en Juridische zaken.

0001

Datum
28 januari 2025

Ons kenmerk
2025-000652

onafhankelijk over het al dan niet verlenen van een ontheffing op de geheimhoudingsplicht ten behoeve van een integriteitsonderzoek. Het instellen van deze commissie is een belangrijke waarborg.
Naast deze waarborg zullen ook aanvullende waarborgen in de beleidsregel moeten worden opgenomen. Waarborgen waaraan gedacht kan worden zijn onder andere: een beschrijving in welke gevallen er een verzoek tot opheffing geheimhouding in het kader van het fiscale integriteitsbeleid kan worden gedaan, wat de bevoegdheid en precieze rol van de adviescommissie is, de juridische status van het besluit op een verzoek tot opheffing geheimhouding en de mogelijke rechtsmiddelen die daartegen openstaan, een beschrijving van de gegevensverwerking in alle fases van het proces, hoe de eisen van proportionaliteit en subsidiariteit hierin worden meegewogen, om wat voor categorieën persoonsgegevens het gaat (soort, aard, hoeveelheid, over welke periode), hoe en op welk moment in het proces de betrokkene geïnformeerd wordt, welke bewaartermijnen gelden, hoe de betrokkene zijn privacyrechten kan uitoefenen en of er sprake is van een uitzondering op de rechten van de betrokkene of plichten van de verwerkingsverantwoordelijke uit hoofde van artikel 23 van de AVG.

Als een deugdelijke beleidsregel is opgesteld, kan weer gestart worden met de verwerking.

Een afschrift van deze brief wordt gedeeld met uw functionaris gegevensbescherming.

Met vriendelijke groet
Autoriteit Persoonsgegevens
Namens deze,

Persoonsgegevens

Programmadirecteur