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
T.a.v. Persoonsgegevens
Persoonsgegevens
Korte Voorhout 7
2511 CW DEN HAAG

Datum
10 december 2024

Ons kenmerk
2024-035022

Contactpersoon
Persoonsgegevens

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 de 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.

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.

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 FG van 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,

Persoonsgegevens