AP | bescherming in een digitale wereld

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

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

Datum
11 september 2025

Ons kenmerk
2024-035022

Contactpersoon
Persoonsgegevens

Onderwerp
Proces afhandeling van gemelde datalekken door Belastingdienst

Geachte Persoonsgegevens

Inleiding
In de periode september 2024 tot en met december 2024 hebben gesprekken plaatsgevonden tussen de Autoriteit Persoonsgegevens (AP) en functionarissen binnen de Belastingdienst die betrokken zijn bij de afhandeling van meldingen van datalekken door de Belastingdienst. Ook is aanvullend informatie verstrekt over de gedocumenteerde werkwijze van de Belastingdienst bij de afhandeling van meldingen van datalekken.

De AP heeft op basis van alle verkregen informatie op 10 december 2024 een brief met vijf verbeterpunten voor de afhandeling van datalekken verstuurd naar de Belastingdienst. De Belastingdienst heeft bij brief van 28 mei 2025 aangegeven hoe de aanbevelingen worden opgevolgd. Over de inhoud van deze brief heeft in juli 2025 nog aanvullend contact met de betrokken medewerkers plaatsgevonden.

Conclusie en doel van deze brief
De AP stelt vast dat de schriftelijke aanbevelingen van 10 december 2024 consistent zijn opgepakt door de Belastingdienst. Tot deze conclusie komt de AP op basis van de beschreven aanpassingen in de werkwijze in de brief van 28 mei 2025 en op basis van de aanvullende toelichting.

De aangegeven verbeterpunten omtrent het registreren van het BSN van een melder, controle op de

volledigheid van veiligheidsincidenten als datalek en het betrekken van de FG zijn consequent opgevolgd en vertaald in concrete vervolgacties. De AP heeft bovendien een concrete indruk gekregen van de termijnen waarop deze aangekondigde maatregelen effectief zijn geworden.

In deze brief worden de ingezette maatregelen benoemd. De AP beëindigt hiermee het toezichttraject voor wat betreft de naleving van de meldplicht datalekken, als onderdeel van het programma van toezicht voor de Belastingdienst. De AP zal de ontwikkelingen op het punt van datalekken blijven volgen.

Toelichting op de conclusie

Opvolging aanbeveling 1: niet meer registeren van het BSN van de melder
Het BSN van een melder wordt niet langer geregistreerd bij het behandelen van een gemeld datalek bij de melddesk datalekken. Het daartoe bestemde dataveld is inmiddels verwijderd uit het programma dat voor de ontvangst en registratie van datalekken in gebruik is. Sinds 1 maart 2025, tot het moment van schrappen in juni 2025, werd het BSN steeds handmatig verwijderd uit het meldformulier door de behandelaars van de meldingen binnen de melddesk datalekken.

Opvolging aanbeveling 2: bewustwording
Aan de bewustwording van de omgang met gevoelige persoonsgegevens door medewerkers wordt voortdurend gewerkt. Iedere (nieuwe) medewerker moet een online game voltooien. Deze game bevat ook vragen over het gegevensbeschermingsrecht. De Belastingdienst heeft de actualiteit van de vragen in de game in juli 2025 gecontroleerd. Op dit moment bestaat geen noodzaak voor verdere inhoudelijke aanpassingen van de game. De huidige invulling van de game verloopt in augustus 2026. Momenteel loopt er een aanbestedingsprocedure ter vervanging van het systeem. Eventuele (significante) aanpassingen van de game vinden plaats in 2026.

Opvolging aanbeveling 3: controle op volledigheid met registraties securityincidenten
Sinds 1 juli 2024 worden alle damages door de Melddesk Datalekken getoetst op de vraag of het een datalek is en bij een bevestigend antwoord in behandeling genomen als een datalek. De damages worden ook allemaal als zodanig in het incidentenregister vermeld, inclusief de afweging of het een datalek betreft en of het datalek gemeld moet worden bij de AP.

Opvolging aanbeveling 4: betrek de FG, bij twijfel over de meldplicht datalekken
De Belastingdienst heeft in de procedure 'Meldplicht datalekken' een aanpassing aangebracht in de werkwijze om de FG op een vaste en gedocumenteerde werkwijze te betrekken bij een datalek, wanneer er twijfel of onduidelijkheid bestaat over de ernst van de gevolgen van een datalek voor de betrokkene(n). Deze procedurele aanpassing behelst dat bij twijfel over de opvolging van de meldplicht voortaan *door of namens de CPO* met de FG wordt gesproken over de inhoud van het beveiligingsincident, waarna het advies van de FG separaat in het registratieprogramma wordt opgenomen. Het betreft een concretisering van de rol van de CPO in het kader van de samenwerking met de FG in geval van twijfel over de (juridische) aspecten van een beveiligingsincident. In het kader van de structurele aanpassing van de werkwijze is het registratieprogramma allereerst aangevuld met een speciaal dataveld, waarin rapportages, selecties en aanvullende informatie door de melddesk datalekken, of namens de CPO, opgenomen kunnen worden voor de uitoefening van de taken van de FG. Per 1 maart 2025 is ook nog een tweede opmerkingenveld aan het registratieprogramma toegevoegd, waarin door medewerkers van de melddesk datalekken wordt

opgenomen of, en volgens welke afweging, een advies aan de FG is gevraagd en, indien bevestigend, of het advies van de FG is opgevolgd door de medewerkers van de melddesk datalekken. Aandachtspunt daarbij blijft wel dat de geadresseerde(n) van de FG-adviezen niet te allen tijde de medewerkers van de melddesk datalekken zelf zijn, maar ook interne organisatieonderdelen betreffen. Het succesvol effectueren van het advies van de FG vergt dat medewerkers van de melddesk datalekken goed overzien, en zo nodig nagaan en documenteren, wat er met de adviezen van de FG gebeurt.

Aanbeveling 5: betrek de FG, indien de directeur afwijkt van het advies van de melddesk datalekken
De melddesk datalekken kan, bij het opvolgen van een ontvangen melding, een advies uitbrengen aan een directie binnen de organisatie om de betrokkene(n) te informeren. Indien een directeur vervolgens afwijkt van het advies om te melden aan de betrokkene(n), dan neemt de melddesk datalekken contact op met de CPO. De CPO beoordeelt vervolgens de situatie en neemt bij twijfel telefonisch contact op met de FG en vraagt advies aan de FG. Dit advies van de FG zal vervolgens schriftelijk gegeven worden en vervolgens vastgelegd worden in het registratieprogramma. Voor het documenteren van deze mogelijke stappen is ook een extra opmerkingenveld toegevoegd in het registratieprogramma. Ook op deze nieuwe afspraken is het werkproces voor het registratieprogramma technisch aangepast. Daarnaast is er een escalatieladder binnen de organisatie ontwikkeld, indien het melden van betrokkenen ten onrechte achterwege blijft.

Geen melding aan de AP in geval van encrypted devices, wél opname in het incidentenregister
Tot slot dient hier ook nog benoemd te worden dat ontvangen meldingen over in het ongewis geraakte encrypted mobiele devices wel dienen te worden vastgelegd als beveiligingsincident in het incidentenregister, maar niet langer gemeld aan de AP als een mogelijk datalek. Mits de versleuteling passend is, rekening houdend met de norm van artikel 32 van de AVG, en de Belastingdienst beschikt over actuele kopieën of back-ups van de persoonsgegevens die op de vermiste encrypted mobiele device staan.

Tot slot

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

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