Belastingdienst

Belastingdienst, Postbus 30206, 2500 GE Den Haag

Grote ondernemingen
Kantoor Rotterdam

Bezoekadres:
Laan op Zuid 45
3072 DB Rotterdam

Postadres:
Postbus 30206
2500 GE Den Haag

Datum
20 april 2021

Behandeld door

Onze referentie

Betreft: *Besluit op Wob-verzoek d.d. 19 januari 2021 inzake omgang met persoonsgegevens en andere vertrouwelijke informatie van belastingplichtigen*
Uw referentie:

Geachte ,

Op 20 januari 2021 ontving de Belastingdienst uw verzoek inzake de Wet Openbaarheid Bestuur (hierna: Wob), gedateerd op 19 januari 2021, waarin u om openbaarmaking van documenten verzoekt inzake de omgang met persoonsgegevens en andere vertrouwelijke informatie van belastingplichtigen binnen het ministerie van Financiën dan wel binnen de Belastingdienst.

Wij hebben uw verzoek in behandeling genomen. Per brief van 11 februari 2021 is door ons de beslistermijn verlengd met toepassing van artikel 6 lid 2 WOB.

Wettelijk kader

Uitgangspunt van de WOB is dat, in het belang van een goede en democratische bestuursvoering, degene die om informatie verzoekt een recht op openbaarmaking van die informatie heeft. Volgens artikel 3 van de WOB ziet de openbaarmaking op gegevens die zijn vastgelegd in documenten, voor zover deze nog niet openbaar zijn (gemaakt). Het bestuursorgaan kan evenwel besluiten om op grond van de artikelen 10 en/of 11 van de WOB of een geheimhoudingsplicht documenten (gedeeltelijk) niet openbaar te maken.

Inhoud van uw verzoek

In uw verzoek geeft u aan dat u verzoekt om documenten inzake de omgang met persoonsgegevens en andere vertrouwelijke informatie van belastingplichtigen binnen het ministerie van Financiën dan wel binnen de Belastingdienst. Op 24 februari 2021 hadden wij telefonisch contact om uw verzoek nader te preciseren. Daaruit kwam naar voren dat u met name op zoek bent naar documenten waaruit blijkt hoe de Belastingdienst omgaat met persoonsgegevens en andere vertrouwelijke documenten.

Grote ondernemingen
Kantoor Rotterdam

Datum
20 april 2021

Onze referentie
[redacted]

Inventarisatie

U heeft uw verzoek onderverdeeld in een vijftal sub-onderwerpen waarover u om openbaarmaking van documenten verzoekt. Wij stellen vast dat deze sub-onderwerpen zien op het beleid van de Belastingdienst met betrekking tot de uitvoering van de Algemene Verordening Gegevensbescherming (hierna: AVG) en artikel 67 van de Algemene wet inzake rijksbelastingen (hierna: AWR). Wij hebben onderzocht of er binnen de organisatie van de Belastingdienst documenten aanwezig zijn die zien op de uitvoering van de hiervoor genoemde regelgeving. Daarbij hebben wij documenten aangetroffen die zien op de melding van het lekken van gegevens van natuurlijke personen.

Beoordeling

De gevonden documenten kunnen openbaar gemaakt worden.

Een deel van de documenten is onleesbaar gemaakt omdat het gegevens bevat die te herleiden zijn tot een persoon. Per melding in het datalekregister is een intern dossier aanwezig dat niet voor openbaarmaking in aanmerking komt gezien artikel 10 lid 1 letter d WOB.

Beslissing

Gelet op het bovenstaande wijzen wij uw verzoek gedeeltelijk toe.[1]

Hoogachtend,

namens de staatssecretaris van Financiën,

de directeur Belastingdienst Grote Ondernemingen,

[redacted]

[1] Dit besluit is een besluit in de zin van de Algemene wet bestuursrecht. Op grond van die wet kunt u tegen dit besluit binnen zes weken na de dag waarop dit besluit is bekendgemaakt een bezwaarschrift indienen. Het bezwaarschrift richt u aan de staatssecretaris van Financiën, ter attentie van ondergetekenden, Postbus 30206, 2500 GE Den Haag.. Het bezwaarschrift dient te worden ondertekend en dient ten minste de volgende gegevens te bevatten:
a. naam en adres van de indiener;
b. de dagtekening;
c. een omschrijving van het besluit waartegen het bezwaar zich richt;
d. de gronden waarop het bezwaar rust.

BIJLAGEN BIJ WOB-BESLUIT

1. Informatie melding datalekken (intranet Belastingdienst)
2. Nieuwe procedure bij datalekken (intranet Belastingdienst)
3. Privacy en AVG (intranet Belastingdienst)
4. Procedure meldplicht datalekken (versie 19 september 2019)
5. Verantwoord omgaan met gegevens (intranet Belastingdienst)
6. Uittreksel datalekregister

Grote ondernemingen
Kantoor Rotterdam

Datum
20 april 2021

Onze referentie
90821.5746.1.0

Nieuwe procedure bij datalekken

Publicatiedatum 28-05-2020, 17:06 | Laatste update 04-06-2020, 8:58 | MEDEDELINGEN

BEVEILIGING - De vernieuwde procedure voor de behandeling van een datalek is gepubliceerd. Het ministerie en de Belastingdienst hanteren nu dezelfde procedure bij datalekken. In de procedure is de rol van de dienstonderdelen duidelijker omschreven. Daar zijn datacoördinatoren beschikbaar voor advies.

Als je denkt te maken te hebben met een datalek, dan moet je dit direct melden bij de Melddesk Datalekken Belastingdienst. Dit kan telefonisch via 888, of per mail naar de postbus van de Melddesk Datalekken Belastingdienst. Informeer ook altijd je leidinggevende. Je leidinggevende bepaalt hoe de directeur wordt geïnformeerd.

Wat doet de melddesk

De melddesk analyseert of het incident moet worden gemeld bij de Autoriteit Persoonsgegevens. Om dat te bepalen zal de melddesk vaak contact opnemen met het dienstonderdeel waar het incident is ontstaan of dat het klantcontact heeft met de klant die het heeft gemeld.

Er is sprake van een datalek als een persoonsgegeven in onbevoegde hand komt, verloren gaat of ontoegankelijk wordt. Dit kan gaan om gegevens van een groot aantal personen of om meerdere gegevens van één persoon of een combinatie daarvan. Daarbij kan sprake zijn van een systeemfout, maar ook een menselijke fout, zoals een fout bij het verzenden van een e-mail of poststukken.

Rol datacoördinator

Elk dienstonderdeel heeft nu ook een datacoördinator die vragen beantwoordt over datalekken, meldingen en de procedure. De datacoördinator staat het dienstonderdeel bij als er herstel- of verbetermaatregelen nodig zijn. Hij adviseert bijvoorbeeld over de juiste vorm van een bericht aan betrokkenen.

Contactpersoon

Ook stelt ieder dienstonderdeel voor elk datalek een contactpersoon aan. Deze wordt door de melddesk geïnformeerd en kan binnen het dienstonderdeel een nadere analyse laten uitvoeren op het incident en zorgt ook voor verdere communicatie binnen het dienstonderdeel.

Vragen?

Voor algemene vragen kun je terecht bij de datacoördinator of bij de Melddesk Datalekken Belastingdienst.

Lees ook de procedure datalekken.

Melddesk Datalekken Belastingdienst

Publicatiedatum 25-03-2019, 14:04 | Laatste update 18-01-2021, 11:02 |

- Organisaties en overheden zijn op grond van de Algemene Verordening Gegevensbescherming (afgekort AVG) verplicht om bij inbreuken met persoonsgegevens maatregelen te nemen om de gevolgen voor degene die betrokken zijn door zo'n inbreuk te beperken of op te heffen. Ook is het verplicht om melding te doen van incidenten met persoonsgegevens bij de Autoriteit Persoonsgegevens. Naast de melding aan de Autoriteit Persoonsgegevens is het in veel gevallen verplicht om hen die betrokken zijn geworden in het datalek te informeren. De "betrokkene" is de wettelijke term voor degene wiens gegevens onjuist zijn verwerkt, gelekt of verloren gegaan.
- Om aan deze verplichtingen te kunnen voldoen heeft de Belastingdienst een Melddesk ingericht. Kortweg MDB genoemd. De MDB beoordeelt alle meldingen van (beveiligings-) incidenten op inbreuken met persoonsgegevens. Op basis van de feiten en omstandigheden wordt een beoordeling van de risico's voor betrokkenen gemaakt. Indien dit leidt tot meldplicht wordt de melding binnen 72 uur gedaan bij de Autoriteit Persoonsgegevens.

Alert zijn op datalekken, direct melden

- Om aan deze termijn van 72 uur te kunnen voldoen, moeten alle medewerkers alert zijn op datalekken en deze direct melden (op dag 1 van het incident), ook buiten kantoortijden. Je meldt dit telefonisch bij 888 (servicedesk 088-15 88 888) of via de e-mail bij de postbus Melddesk Datalekken Belastingdienst.
- De MDB coördineert de afhandeling van een datalek. De directeur van het betrokken organisatieonderdeel wordt geïnformeerd, het organisatieonderdeel wordt ingelicht. De MDB helpt ook bij het opstellen van een bericht aan betrokkene. Het bericht aan de betrokkene wordt verzorgd door het organisatieonderdeel omdat dit dan gecombineerd kan worden met de herstelacties(s).
- De MDB signaleert trends om ook samen met het organisatieonderdeel te beoordelen of verbeteringen kunnen worden aangebracht. De medewerkers kunnen adviseren ingeval van twijfel, dus schroom niet de MDB te raadplegen.
- Wil je meer informatie over de procedure lees dan via deze link de procedure Datalekken AVG Belastingdienst.
- Voorbeelden van datalekken zijn:
  - Het lekken van persoonsgegevens door bijvoorbeeld dossiers of gegevensdragers te verliezen zoals laptops, smartphones en tablets.
  - Dit kan ook ontstaan door inbraken op het systeem (hacken) of op sites van de dienst, die worden gesignaleerd door het Secure Operations Centre.
  - Veel datalekken ontstaan door het onjuist verzenden van gevoelige gegevens doordat een e-mail of een brief aan een onjuiste wordt gezonden of ter hand gesteld. Door een extra check bij verzending kan dit worden voorkomen.
- Wil je informatie verkrijgen of voorlichting in je team of afdeling over de werkwijze van de MDB of voor het maken van afspraken voor je organisatieonderdeel kun je contact opnemen met de coördinator van MDB ( ) per e-mail of telefoon 06- .

Nieuwe procedure bij datalekken

Publicatiedatum 28-05-2020, 17:06 | Laatste update 04-06-2020, 8:58 | MEDEDELINGEN

BEVEILIGING - De vernieuwde procedure voor de behandeling van een datalek is gepubliceerd. Het ministerie en de Belastingdienst hanteren nu dezelfde procedure bij datalekken. In de procedure is de rol van de dienstonderdelen duidelijker omschreven. Daar zijn datacoördinatoren beschikbaar voor advies.

Als je denkt te maken te hebben met een datalek, dan moet je dit direct melden bij de Melddesk Datalekken Belastingdienst. Dit kan telefonisch via 888, of per mail naar de postbus van de Melddesk Datalekken Belastingdienst. Informeer ook altijd je leidinggevende. Je leidinggevende bepaalt hoe de directeur wordt geïnformeerd.

Wat doet de melddesk

De melddesk analyseert of het incident moet worden gemeld bij de Autoriteit Persoonsgegevens. Om dat te bepalen zal de melddesk vaak contact opnemen met het dienstonderdeel waar het incident is ontstaan of dat het klantcontact heeft met de klant die het heeft gemeld.

> Er is sprake van een datalek als een persoonsgegeven in onbevoegde hand komt, verloren gaat of ontoegankelijk wordt. Dit kan gaan om gegevens van een groot aantal personen of om meerdere gegevens van één persoon of een combinatie daarvan. Daarbij kan sprake zijn van een systeemfout, maar ook een menselijke fout, zoals een fout bij het verzenden van een e-mail of poststukken.

Rol datacoördinator

Elk dienstonderdeel heeft nu ook een datacoördinator die vragen beantwoordt over datalekken, meldingen en de procedure. De datacoördinator staat het dienstonderdeel bij als er herstel- of verbetermaatregelen nodig zijn. Hij adviseert bijvoorbeeld over de juiste vorm van een bericht aan betrokkenen.

Contactpersoon

Ook stelt ieder dienstonderdeel voor elk datalek een contactpersoon aan. Deze wordt door de melddesk geïnformeerd en kan binnen het dienstonderdeel een nadere analyse laten uitvoeren op het incident en zorgt ook voor verdere communicatie binnen het dienstonderdeel.

Vragen?

Voor algemene vragen kun je terecht bij de datacoördinator of bij de Melddesk Datalekken Belastingdienst.

Lees ook de procedure datalekken.

Privacy en Algemene Verordening en Gegevensbescherming (AVG)

Publicatiedatum 25-03-2019, 14:02 | Laatste update 27-08-2020, 11:31 |

Gegevensverwerking is een belangrijke pijler voor onze organisatie en verwerkt miljoenen gegevens die veelal te relateren zijn aan personen. Het eigenaarschap, de kwaliteit, de bescherming van privacy en het voorkomen van datalekken vormen belangrijke vraagstukken voor nu en de toekomst. De directie IV-en databeheersing geeft hiervoor kaders.

De organisatie kent een zware verantwoordelijkheid om zorgvuldig met gegevens van burgers en bedrijven maar ook van haar eigen medewerkers om te gaan. Veel regels zijn bepaald door de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet AVG. Maar andere regels zijn al langer van toepassing. Denk hierbij aan de Wet bescherming politiegegevens (Wbp) en de Algemene beginselen van behoorlijk bestuur. Privacy gaat over rechtmatig en zorgvuldig omgaan met persoonsgegevens. Als organisatie werken we op basis van gemeenschappelijke standaarden, technieken en methoden. IV&D is verantwoordelijk voor het opstellen en onderhouden van deze kaders, en houdt deze in lijn met de rijksbrede kaders.

Waaruit bestaat privacy

Privacy kent verschillende vormen. Hier gaat enkel over informationele privacy: het verwerken van persoonlijke data. Het privacybeleid Financiën is ontwikkeld om binnen ministerie van Financiën sturing te geven aan de bescherming van persoonsgegevens. Het doel hiervan is te zorgen dat onze organisatie voldoet aan de verplichtingen van privacywetgeving zoals de AVG, de WPG en de Algemene beginselen van behoorlijk bestuur. Privacy gaat meer over gedrag dan over procedures, meer over risico's beheren en inzichtelijk maken dan over maatregelen en techniek, meer over 'nog eens nadenken' dan over 'we doen dat altijd al zo'. De AVG stelt de rechten van betrokkene centraal en kijkt naar de risico's die de betrokkene loopt bij de verwerking van zijn of haar gegevens. Ook de invloed van de betrokkene op zijn of haar registratie is groter geworden en zijn of haar autonomie is stevig verankerd in de verordening.

Rol van IV&D

IV&D ontwikkelt in algemene zin de kaderstelling voor privacy. Deze kaderstelling is relevant voor alle bedrijfsonderdelen. Voor de online interactie is dit met name relevant voor de Corporate Dienst Communicatie. Daarnaast is IV&D verantwoordelijk voor kaders omtrent privacyborging van persoonsgegevens van burgers en bedrijven en personeelsgegevens?

IV&D ondersteunt de uitvoerende directies bij processen om de uitoefening door burgers en medewerkers van rechten onder de AVG te verzekeren. Daarnaast ondersteunt IV&D bij het uitvoeren van PIA's en monitoring van de follow up daarvan, en bij het beheer van het door de AVG voorgeschreven register van verwerkingen van persoonsgegevens. Ook fungeert de afdeling als aanspreek- en coördinatiepunt op het gebied van privacy voor het Kerndepartement en de Functionaris Gegevensbescherming (FG).

Beschrijving rollen en verantwoordelijkheden met betrekking tot privacy

Rollen en verantwoordelijkheden

- Chief Information Officer (CIO)
- Beveiligingsambtenaar (BVA)
- Functionaris voor Gegevensbescherming (FG)

Functionaris voor Gegevensbescherming (FG)

Chief Information Security Officer (CISO)

Juridische Zaken (JZ)

Privacy Officer (PO)

Datacoördinator (DC) Belastingdienst

De medewerker

Ministerie van Financiën

Procedure meldplicht datalekken

Ministerie van Financiën
Versie 1.0

Datum 19 september 2019
Status Definitief

Colofon

Titel	Procedure meldplicht datalekken
Auteur(s)	CIO-office kerndepartement DG Belastingdienst Concerndirectie Informatievoorziening en Databeheersing
Bijlagen	3
Inlichtingen	**Kerndepartement:** Directie Bedrijfsvoering/ Eenheid Informatisering/ CIO-office **Belastingdienst** DG Belastingdienst, Concerndirectie Informatievoorziening en Databeheersing

Inhoud

1 Doel

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. Dit houdt in dat bedrijven en overheden die te maken krijgen met een ernstig datalek verplicht zijn dat te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en soms ook bij het getroffen individu, de betrokkene, zowel burger als medewerker. Doel is de gevolgen van een inbreuk met persoonsgegevens voor betrokkene(n) zoveel mogelijk te beperken en bedrijven en organisaties meer bewust te maken van hun verantwoordelijkheden. In 2018 werd de Algemene verordening gegevensbescherming (AVG) van toepassing, met daarin strengere eisen aan de registratie van datalekken. Met ingang van 1 januari 2019 geldt ook voor de Wet Politiegegevens de meldplicht datalekken. De Belastingdienst moet in zijn bedrijfsvoering rekening houden met de AVG en de WPG. Deze procedure meldplicht datalekken geldt voor het gehele Ministerie van Financiën, inclusief alle dienstonderdelen van de Belastingdienst, en doet recht aan zowel AVG als WPG.

In dit gezamenlijke document zijn de procedures van het kerndepartement en de Belastingdienst samengebracht tot één gemeenschappelijke procedure voor het Ministerie van Financiën. In de bijlagen staan afzonderlijke werkinstructies.

Bij een datalek[1] gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens en verlies van (toegang tot) persoonsgegevens.[2]

Een datalek hoeft niet in alle gevallen te worden gemeld bij de AP. Elk incident moet individueel worden beoordeeld. Alleen als het waarschijnlijk is dat het incident een risico inhoudt voor de rechten en vrijheden van natuurlijke personen moet het datalek worden gemeld. Heeft de inbreuk ook waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene(n), dan moet de organisatie ook de betrokkene(n) informeren. Als er geen melding wordt gemaakt van een datalek, kan dit bestraft worden met een bestuurlijke boete.

Een datalek dient zonder onredelijke vertraging te worden gemeld. Dit houdt in dat uiterlijk 72 uur[3] nadat de organisatie/verwerkingsverantwoordelijke heeft kennisgenomen van het datalek de AP en eventueel ook de betrokkene moet worden geïnformeerd. Het melden binnen 72 uur maakt dat een organisatie, na het ontdekken van het datalek, enige tijd mag nemen voor nader onderzoek.

Deze procedure beschrijft hoe te handelen en welke stappen moeten worden genomen binnen het ministerie van Financiën4, inclusief de Belastingdienst, indien er sprake is van een datalek of wanneer een datalek vermoed wordt.
Het volgende resultaat wordt hiermee nagestreefd.

1 De term datalek komt niet voor in de AVG en de WPG. In plaats daarvan wordt gesproken over een 'inbreuk in verband met persoonsgegevens': een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.
2 Definitie overgenomen van Autoriteit Persoonsgegevens.
3 Deze 72 uur geldt ongeacht of er sprake is van een werkdag, zaterdag, zondag of feestdag.
4 Dit document is opgesteld door het kerndepartement en de Belastingdienst. Waar in dit document Ministerie van Financiën staat, wordt bedoeld het ministerie inclusief de Belastingdienst, tenzij anders benoemd.

- Het zorgvuldig waarborgen van de belangen van betrokkenen bij een (mogelijk) datalek en het beperken van de gevolgen van datalekken voor de betrokkenen;
- Het zorgvuldig waarborgen van de belangen van het ministerie bij een (mogelijk) datalek en het beperken van de gevolgen van datalekken voor het ministerie dan wel een andere organisatie die betrokken is;
- Het steeds volgen van een eenduidige procedure;
- Het op zorgvuldige en systematische wijze analyseren van het (mogelijke) datalek;
- Het borgen van een uniforme rapportage aan de betrokkene, de verwerkingsverantwoordelijke en de toezichthouder.

2 Toepassingsgebied en beheer procedure

De procedure meldplicht datalekken geldt voor alle departementsonderdelen van het ministerie van Financiën waar de minister van Financiën verwerkingsverantwoordelijke voor is.

Deze procedure beschrijft de uitgangspunten, principes en processtappen waar het ministerie zich aan dient te houden. Om nadere invulling te kunnen geven aan de processtappen zijn afzonderlijke werkinstructies opgesteld voor het kerndepartement en de Belastingdienst. Reden hiervoor is dat er (vooralsnog) voor is gekozen om vanwege de schaalgrootte van de Belastingdienst binnen het ministerie twee 'meldpunten datalekken' in te richten: één bij het kerndepartement onder de verantwoordelijkheid van de CIO-office van het kerndepartement en één bij de Belastingdienst onder de verantwoordelijkheid van de concerndirectie Informatievoorziening en Databeheersing (IV&D). Als basisprincipe geldt dat de meldpunten dezelfde uitgangspunten hanteren en processtappen volgen. De invulling van de rollen en verdeling van de verantwoordelijkheden binnen het proces kunnen echter van elkaar verschillen. Deze laatste punten worden in de werkinstructies uitgewerkt (zie bijlagen).

Domeinen Roerende Zaken (DRZ) meldt mogelijke datalekken bij het Meldpunt Datalekken van het kerndepartement.

De ZBO's, zoals opgenomen in het openbare ZBO-register, vallen buiten het bereik van deze procedure.

De departementale Chief Information Officer (CIO) van het ministerie van Financiën is verantwoordelijk voor het vaststellen van de procedure meldplicht datalekken. Hierbij wordt hij ondersteund door de CIO-offices van het kerndepartement (KD) en de Belastingdienst (BD).

De procedure meldplicht datalekken van het ministerie van Financiën wordt minimaal één keer per drie jaar, of zodra daartoe aanleiding is (bijvoorbeeld majeure wijzigingen in de wetgeving) geëvalueerd en zonodig bijgesteld. De procedure maakt deel uit van het privacybeleid van het ministerie van Financiën[5]. Voor de governance (besturing) van de privacyorganisatie wordt verwezen naar het privacybeleid.

5 Zie hiervoor: Privacybeleid Financiën, pm link

3 Uitgangspunten en principes

Het ministerie van Financiën hanteert de onderstaande uitgangspunten en principes ten aanzien van de procedure meldplicht datalekken.

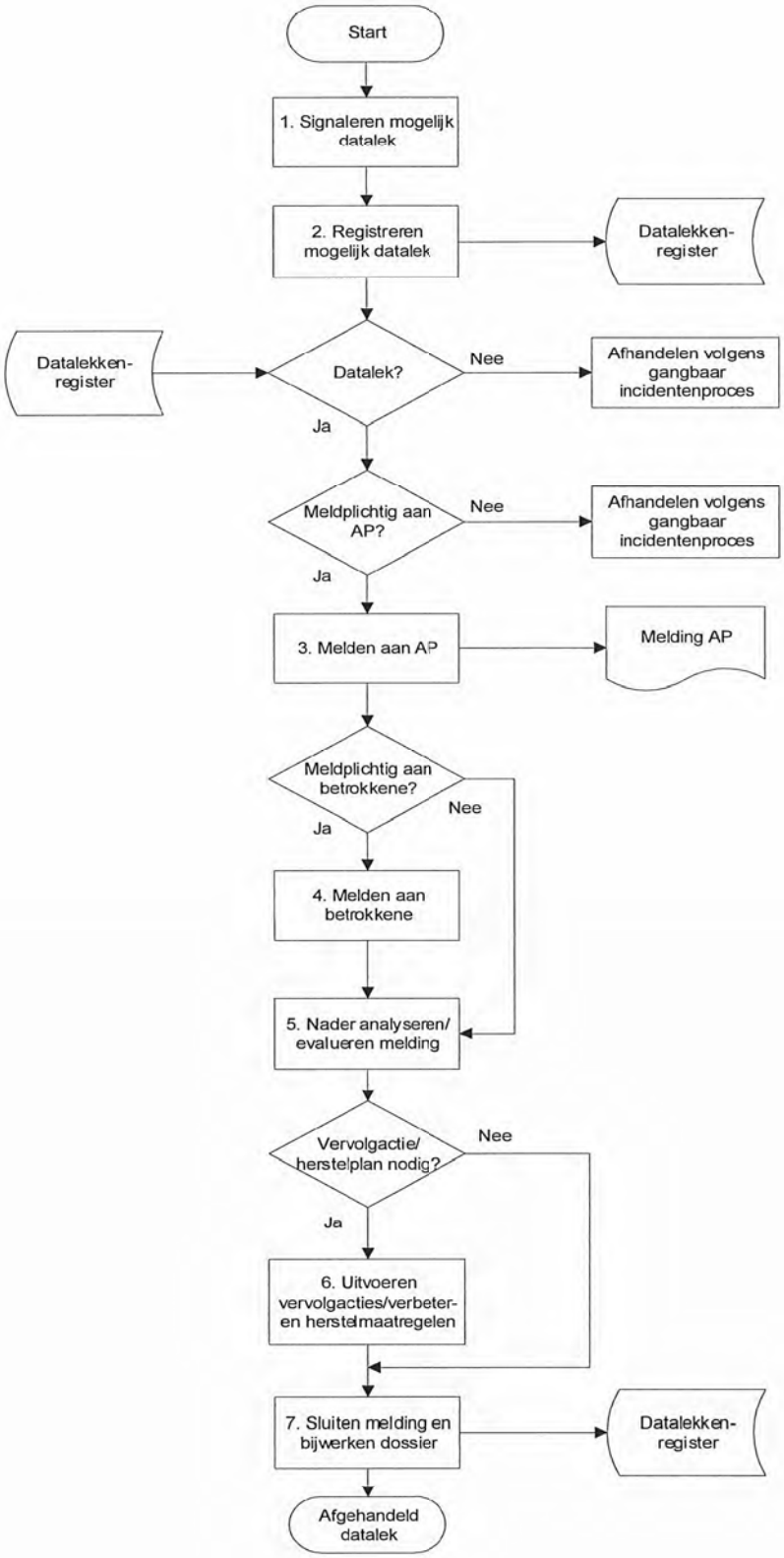
- Het kerndepartement en de Belastingdienst hebben elk een Meldpunt Datalekken ingericht. Zowel het kerndepartement als de Belastingdienst hebben een afzonderlijke werkinstructie meldplicht datalekken. DRZ maakt een aanvulling op de werkinstructie van het kerndepartement;
- Iedere medewerker van het ministerie van Financiën die kennisneemt van een incident waarbij mogelijk sprake is van een datalek moet hiervan zonder enige vertraging melding doen bij een centraal meldpunt en zijn/haar leidinggevende. In de afzonderlijke werkinstructies wordt nader uitgewerkt waar een medewerker de melding moet indienen;
- Bij gegevensverwerking onderscheid je verwerkingsverantwoordelijken en verwerkers van gegevens. De meldplicht rust op de verwerkingsverantwoordelijke(n). De minister van Financiën is verantwoordelijk voor alle (persoons)gegevens die hij voor zijn taak gebruikt. Een verwerker, bijvoorbeeld P-Direkt of Doc-Direkt, is verplicht het ministerie van Financiën zonder onredelijke vertraging te informeren over datalekken, zodat laatstgenoemde de melding op tijd kan doen. Afspraken hierover moeten in verwerkersovereenkomsten of verwerkersafspraken worden vastgelegd. Ook moet zijn afgesproken hoe een verwerker een incident meldt bij de verwerkingsverantwoordelijke;
- Het is echter ook mogelijk dat het ministerie van Financiën verwerker is van persoonsgegevens. In dat geval is het organisatieonderdeel dat de verwerking uitvoert, verplicht een mogelijk datalek zonder enige vertraging te melden bij de (externe) verwerkingsverantwoordelijke. Hoe deze melding moet worden uitgevoerd, wordt eveneens in een verwerkersovereenkomst vastgelegd;
- Iedere melding over een mogelijk datalekincident wordt geregistreerd in een centraal overzicht; het register voor datalekken. Dit geldt ook voor de meldingen die plaatsvinden bij verwerkers. Het incident, de gevolgen, de opvolging ervan en de genomen corrigerende maatregelen moeten in het register worden vastgelegd. Ook motivaties achter beslissingen worden vastgelegd in het register, zoals voor het niet doen van een melding;
  De registratie wordt 3 jaar bewaard ten behoeve van rapportage en verantwoording;
- De AP moet over een datalek worden geïnformeerd uiterlijk 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen.

4 Procedure

Voor het afhandelen van beveiligingsincidenten en datalekken binnen het ministerie van Financiën worden onderstaande processtappen gevolgd.

1. Signaleren mogelijk datalek
2. Registeren mogelijk datalek
3. Melden aan de Autoriteit Persoonsgegevens (AP)
4. Melden aan betrokkene
5. Nadere analyse en evaluatie van de melding
6. Uitvoeren vervolgacties, verbeter- of herstelmaatregelen
7. Sluiting van de melding

Na het schematische overzicht, worden per processtap de uit te voeren activiteiten uitgewerkt. Zoals al eerder aangegeven zullen in de werkinstructies voor het kerndepartement en Belastingdienst de stappen verder worden uitgediept.


Start
1. Signaleren mogelijk datalek
2. Registreren mogelijk datalek
Datalekken-register
Datalekken-register
Datalek?
Nee
Afhandelen volgens gangbaar incidentenproces
Ja
Meldplichtig aan AP?
Nee
Afhandelen volgens gangbaar incidentenproces
Ja
3. Melden aan AP
Melding AP
Meldplichtig aan betrokkene?
Nee
Ja
4. Melden aan betrokkene
5. Nader analyseren/ evalueren melding
Vervolgactie/ herstelplan nodig?
Nee
Ja
6. Uitvoeren vervolgacties/verbeter- en herstelmaatregelen
7. Sluiten melding en bijwerken dossier
Datalekken-register
Afgehandeld datalek

1. Signaleren van een mogelijk datalek.

- Een mogelijk datalek kan op vele manieren worden gesignaleerd, waaronder door de medewerkers van Financiën, maar ook door burgers, andere (rijks)overheidsorganisaties zoals SSC ICT en NCSC, of derden.
- Een incident waarbij sprake is van een (mogelijk) datalek wordt onmiddellijk gemeld bij de CISO (kerndepartement) of het Meldpunt Datalekken (Belastingdienst), zie hiervoor de werkinstructies. Bij de melding wordt aangeven wat voor soort incident het betreft (zoals verlies van dossiers, gegevensdragers en apparatuur zoals laptop, smartphone en tablet), maar ook inbreuken op systemen en diefstal vanuit gebouwen.
- Een medewerker meldt het mogelijke datalek ook bij zijn/haar leidinggevende.

2. Registreren mogelijk datalek

- Het Meldpunt Datalekken registreert de melding in het datalekkenregister en categoriseert deze als een (mogelijk) datalek. Hierbij worden minimaal de volgende gegevens opgenomen6.
  - Aard van de inbreuk;
  - De datum en het tijdstip van het datalek of het incident en van het moment van de ontdekking van het datalek;
  - De verantwoordelijke van de desbetreffende verwerking;
  - De contactpersonen van de inbreuk;
  - Een omschrijving van de gelekte gegevensset (of een inschatting hiervan);
  - Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
  - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om deze gevolgen te verhelpen;
  - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om dergelijke incidenten in de toekomst te voorkomen;
  - Een samenvatting van de eventuele communicatie met de toezichthoudende autoriteit en de betrokkene(n);
  - Datum en tijdstip van de melding aan de toezichthoudende autoriteit en betrokkene, indien verplicht.
- Gedurende de doorlooptijd van de melding wordt de status bijgehouden in het datalekkenregister. Indien nodig wordt een dossier aangelegd.
- Het Meldpunt Datalekken beoordeelt en bepaalt aan de hand van de richtlijnen van de Europese Toezichthouders[7] of er sprake is van een inbreuk op de beveiliging van persoonsgegevens (zie schema in de bijlage).
  De volgende gevallen zijn mogelijk:
  a. Er is geen inbreuk. Het betreft geen datalek en er wordt niet gemeld aan de AP. De motivering wordt opgenomen in het Datalekkenregister. De melding wordt verder afgehandeld via het gangbare incidentmanagementproces.
  b. Er is wel een inbreuk en het beveiligingsincident wordt geclassificeerd als een datalek.

3. Melden aan de Autoriteit Persoonsgegevens (AP)

- Het Meldpunt Datalekken beoordeelt en bepaalt, zonodig in samenwerking met de privacyofficer en waar nodig met de FG, aan de hand van de richtlijnen van de Europese Toezichthouders of er sprake is van een meldingsplicht aan de AP. De volgende gevallen zijn mogelijk.

6 Zie vragenlijst AP: https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1
7 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

a. Het datalek is niet meldplichtwaardig, er wordt niet gemeld aan de AP. De motivering hiervoor wordt opgenomen in het datalekkenregister. De melding wordt verder afgehandeld via het gangbare incidentmanagementproces.
b. Het datalek is meldplichtwaardig.
Indien het datalek meldplichtwaardig is, zal de CIO of een door de CIO aangewezen medewerker melding doen van het datalek bij de AP aan de hand van het webformulier op de website van de AP. De AP zendt een ontvangstbevestiging. De AP kan om nadere informatie vragen.

- Verloren devices worden gemeld bij de AP.

4. Melden aan betrokkene

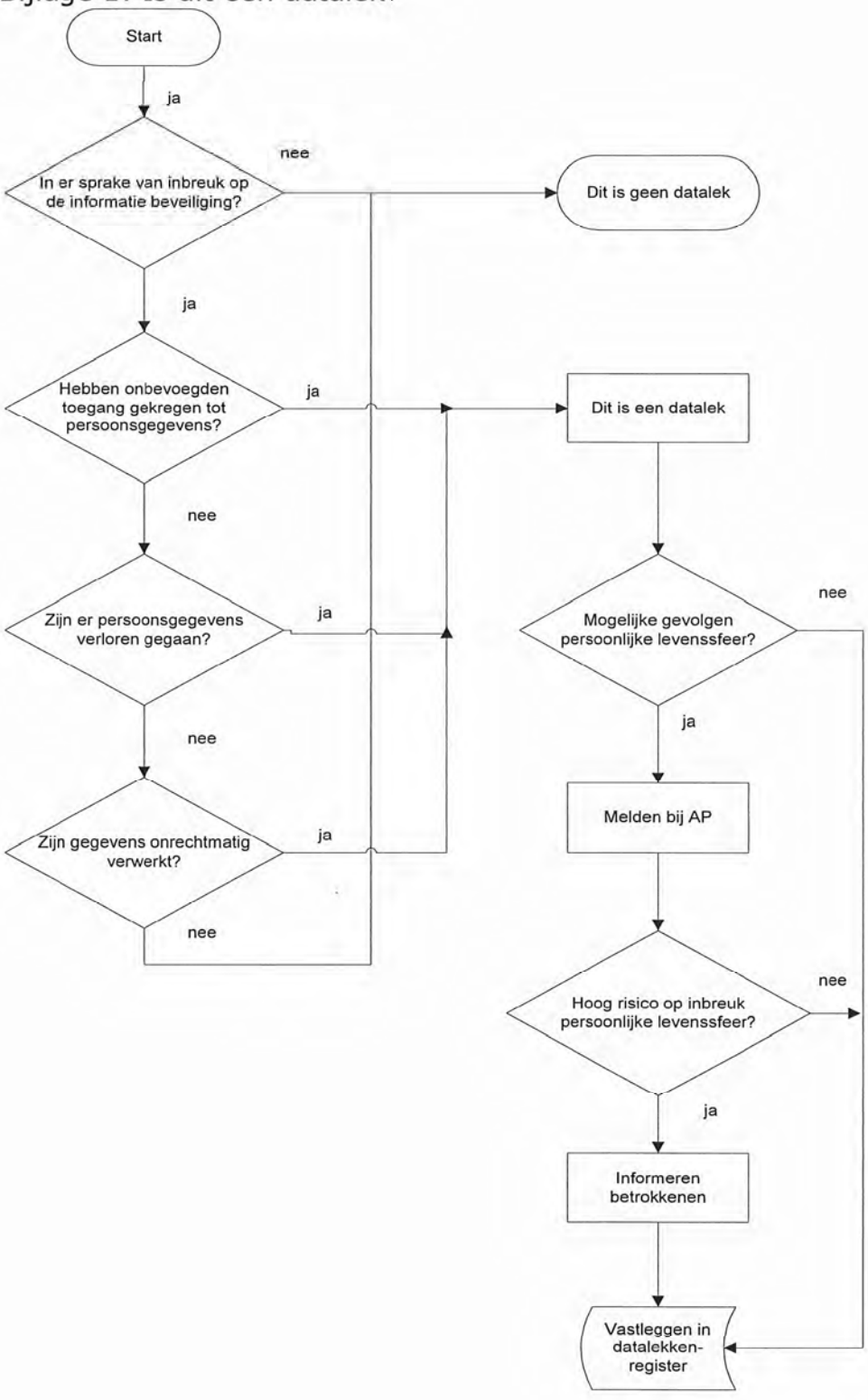
- Het Meldpunt Datalekken beoordeelt en bepaalt, zonodig in overleg met de privacyofficer en waar nodig de FG, aan de hand van de richtlijnen van de Europese Toezichthouders, of er gemeld moet worden aan betrokkene(n).
De volgende gevallen zijn mogelijk.
  a. Er hoeft niet gemeld te worden aan de betrokkene(n). De motivering wordt opgenomen in het Datalekkenregister.
  b. Er moet gemeld worden aan de betrokken(en).
- Een datalek wordt gemeld aan de betrokkene(n) wanneer de inbreuk een waarschijnlijk hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen.
- Deze melding wordt gedaan in duidelijke en eenvoudige taal. In deze melding wordt minimaal de aard van de inbreuk en de genomen maatregelen gecommuniceerd.
- Een dergelijke kennisgeving is niet noodzakelijk wanneer er aan één van de volgende voorwaarden is voldaan.
  - Er zijn technische en organisatorische maatregelen genomen om de persoonsgegevens onbegrijpelijk te maken voor onbevoegden en deze maatregelen zijn toegepast op de persoonsgegevens die gelekt zijn;
  - Er zijn achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van de betrokkenen zich niet voordoet;
  - Een dergelijke mededeling door de verwerkingsverantwoordelijke zou onevenredige inspanningen vergen. In een dergelijk geval kan men kiezen voor een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
  - Indien de gegevens vallen onder de Wet Politiegegevens kan de mededeling aan de betrokkene worden uitgesteld, beperkt of achterwege gelaten:
    - ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
    - ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
    - ter bescherming van de openbare veiligheid;
    - ter bescherming van de rechten en vrijheden van derden;
    - ter bescherming van de nationale veiligheid.
- Indien de betrokkene moet worden geïnformeerd zal de verantwoordelijke lijnmanager dit op zich nemen. Het Meldpunt Datalekken ondersteunt, waar nodig in overleg met de privacyofficer, de lijnmanager hierbij.
- Het geniet de voorkeur om betrokkene(n) op individuele basis te benaderen. Bij meer omvangrijke incidenten kan, in overleg met de privacyofficer, gekozen worden voor algemene voorlichting. De melding aan betrokkene wordt geregistreerd.

5. Nadere analyse en evaluatie van de melding
- Er wordt door de CISO en het Meldpunt Datalekken (en zonodig de privacyofficer en FG) een analyse/evaluatie op de melding uitgevoerd. Het resultaat hiervan wordt vastgelegd in het dossier.
- Mede in het kader van de bewustwording vindt er terugkoppeling plaats naar het betreffende dienstonderdeel en/of de verantwoordelijke voor de procedure.

6. Uitvoeren vervolgacties, verbeter- of herstelmaatregelen
- De CISO (en zonodig de privacyofficer en de FG) onderzoekt of vervolgacties of verbetermaatregelen gewenst zijn.
- Indien het noodzakelijk is om verbetermaatregelen te treffen worden deze uitgevoerd door de verantwoordelijke lijnmanager, waar nodig geadviseerd door de CISO. De CISO stelt zonodig vast dat bestaande kaders niet voldoen, past de kaders in dat geval aan en stelt vast of er aanvullend/aangepast beleid nodig is om het incident in de toekomst te voorkomen.
- De CISO ziet erop toe dat de verbetermaatregelen structureel worden geborgd door de lijnmanager.

7. Sluiting van de melding
- Wanneer de verbetermaatregelen zijn geïmplementeerd of indien er geen vervolgactie noodzakelijk is, sluit het Meldpunt Datalekken de melding af.
- Het Meldpunt Datalekken werkt tot slot het dossier bij.

Bijlage 1: Is dit een datalek?



Toelichting Inbreuk op de informatiebeveiliging
Een inbreuk op de informatiebeveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Voorbeelden van beveiligingsincidenten zijn:

- een kwijtgeraakte USB-stick;
- een gestolen of verloren laptop;
- een inbraak door een hacker;
- een malware- of ransomwarebesmetting;
- het per ongeluk vernietigen van een (papieren) dossier of aangifte;
- het verzenden van een bericht aan de verkeerde belastingplichtige.

Toelichting op Onbevoegdentoegang tot persoonsgegevens
De AVG en de richtlijn spreken in dit verband over inbreuk op de vertrouwelijkheid van persoonsgegevens. In de praktijk komt het erop neer dat persoonsgegevens terecht zijn gekomen bij personen die niet bevoegd zijn om deze gegevens in te zien, te ontvangen of te verwerken. Een verkeerd geadresseerde mail met daarin een dossier met persoonsgegevens is dus een datalek en dient direct gemeld te worden.

Toelichting op Verlies van persoonsgegevens
Verlies houdt in dat de organisatie de persoonsgegevens niet meer heeft. Bij het beveiligingsincident zijn de persoonsgegevens vernietigd of op een andere manier verloren gegaan, en is er geen complete en actuele reservekopie (back-up) van de gegevens. Betreft het hier persoonsgegevens dan is er sprake van een datalek.

Bijlage 2: Werkinstructie meldplicht datalekken Kerndepartement

Inleiding
Vanaf 1 januari 2016 is de meldplicht datalekken van kracht. Dit houdt in dat bedrijven en overheden die te maken krijgen met een ernstig datalek verplicht zijn dat te melden bij de toezichthouder, de Autoriteit Persoonsgegevens (AP) en soms ook bij het getroffen individu, de betrokkene.

Bij een datalek[8] gaat het om toegang tot of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens, en verlies van (toegang tot) persoonsgegevens[9]

Deze werkinstructie beschrijft hoe te handelen en welke stappen moeten worden genomen binnen het kerndepartement van het ministerie van Financiën indien er sprake is van een datalek of wanneer een datalek vermoed wordt.

Governance
De minister is de verwerkingsverantwoordelijke voor alle verwerkingen die onder zijn verantwoordelijkheid worden uitgevoerd. De directeuren(-generaal) zijn gemandateerd om gegevensverwerkingen namens de minister uit te voeren en zijn daarom gemandateerde verwerkingsverantwoordelijken. Het lijnmanagement is verantwoordelijk voor de naleving van privacy en bescherming van de persoonsgegevens binnen de afdeling.

Binnen het kerndepartement wordt de naleving van de meldplicht datalekken ondersteund door de interne privacyorganisatie. Deze organisatie is verwant aan de informatiebeveiligingsorganisatie, zodat daarbij zoveel mogelijk aansluiting is gezocht. Binnen het kerndepartement is een meldpunt voor datalekken ingericht (datalekken@minfin.nl). Dit Meldpunt Datalekken bestaat uit de CISO, de privacy-officer en adviseurs informatiebeveiliging van de CIO-office van het kerndepartement.
Voor een verdere uitwerking van de rollen en verantwoordelijkheden van de privacy-organisatie wordt verwezen naar het privacybeleid van het ministerie[10].

Hierna volgt de werkinstructie meldplicht datalekken voor het kerndepartement. De instructie kent de volgende stappen:
1. Signaleren mogelijk datalek
2. Registeren mogelijk datalek
3. Melden aan de Autoriteit Persoonsgegevens (AP)
4. Melden aan betrokkene
5. Nadere analyse en evaluatie van de melding
6. Uitvoeren vervolgacties, verbeter- of herstelmaatregelen

8 De term datalek komt niet voor in de wet. In plaats daarvan heeft de AVG het over een 'inbreuk in verband met persoonsgegevens': een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens
9 Definitie overgenomen van Autoriteit Persoonsgegevens
10 Zie hiervoor: Privacybeleid Financiën, pm link.

7. Sluiting van de melding

1. Signaleren van een mogelijk datalek.

- Een mogelijk datalek kan op vele manieren worden gesignaleerd, waaronder door de medewerkers van Financiën, maar ook door burgers, andere (rijks)overheidsorganisaties NCSC, leveranciers of derden.
- Iedere medewerker van het kerndepartement die kennis neemt van een incident waarbij mogelijk sprake is van een datalek moet hiervan meteen melding doen
    - Een incident waarbij sprake is van een (mogelijk) datalek wordt onmiddellijk gemeld bide CISO van het kerndepartement:

het Meldpunt Datalekken van het kerndepartement

- De melding kan zowel telefonisch als per e-mail worden doorgegeven.
- Bij de melding dient te worden aangegeven wat voor soort incident het betreft (zoals verlies van dossiers, gegevensdragers, apparatuur (laptop, smartphone en tablet), maar ook inbreuken op systemen en diefstal vanuit gebouwen.

2. Registreren mogelijk datalek

- De Privacy Officer van het kerndepartement registreert de melding in het datalekkenregister en categoriseert deze als een (mogelijk) datalek. Hierbij worden minimaal de volgende gegevens opgenomen:
    - Aard van de inbreuk;
    - De datum en het tijdstip van het datalek of het incident en van het moment van de ontdekking van het datalek;
    - De verantwoordelijke van de desbetreffende verwerking;
    - Contactpersonen omtrent inbreuk;
    - Omschrijving van de gelekte gegevensset (of een inschatting hiervan);
    - Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
    - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om deze gevolgen te verhelpen;
    - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om dergelijke incidenten in de toekomst te voorkomen;
    - Een samenvatting van de eventuele communicatie met de toezichthoudende autoriteit en de betrokkene(n);
    - Datum en tijdstip van de melding aan de toezichthoudende autoriteit en betrokkene, indien verplicht.
- Gedurende de doorlooptijd van de melding wordt de status bijgehouden in het datalekkenregister. Indien nodig wordt een dossier aangelegd.
- De CISO beoordeelt en bepaalt eventueel in samenwerking met het Meldpunt Datalekken aan de hand van de richtlijnen van de Europese Toezichthouders[11] of er sprake is van een inbreuk op de beveiliging van persoonsgegevens (zie schema in de bijlage).

  De volgende gevallen zijn mogelijk:
    a. Er is geen inbreuk in de zin van de AVG (AVG is niet van toepassing of past niet binnen de definitie van een inbreuk). Het betreft geen datalek en er wordt niet gemeld aan de AP. De motivering wordt opgenomen in

11 Zie Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) Nederlandse vertaling:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht_datalekken.pdf

het Datalekkenregister. De melding wordt verder afgehandeld via het gangbare incidentmanagementproces.

b. Er is wel een inbreuk in de zin van de AVG en het beveiligingsincident wordt geclassificeerd als een datalek.

3. Melden aan de Autoriteit Persoonsgegevens (AP)

- De CISO beoordeelt en bepaalt in samenwerking met het Meldpunt Datalekken en zonodig de FG aan de hand van de richtlijnen van de Europese Toezichthouders of er sprake is van een meldingsplicht aan de AP.
  De volgende gevallen zijn mogelijk:
  a. Het datalek is niet meldplichtwaardig, er wordt niet gemeld aan de AP. De motivering hiervoor wordt opgenomen in het datalekkenregister. De melding wordt verder afgehandeld via het gangbare incidentmanagementproces.
  b. Het datalek is meldplichtwaardig.
- Indien het datalek meldplichtwaardig is, zal de CISO melding doen van het datalek bij de AP aan de hand van het webformulier op de website van de AP.
- Medewerkers van het kerndepartement melden een datalek nooit zelf bij de AP.
- De CISO meldt het datalek uiterlijk 72 uur nadat de verwerkingsverantwoordelijke er kennis van heeft genomen bij de AP.
- Het kerndepartement hanteert als stelregel dat de verwerkingsverantwoordelijke nog geen kennisgenomen heeft van het datalek wanneer deze op de hoogte wordt gesteld over een *potentieel* datalek: de verwerkingsverantwoordelijke moet onderzoeken of er sprake is van een datalek en de 72 uur gaan pas tikken *zodra* de verwerkingsverantwoordelijke met redelijke zekerheid gelooft dat er een datalek heeft plaatsgevonden waarbij er persoonsgegevens zijn aangetast (T=0). Het onderzoek moet zo snel mogelijk plaatsvinden.

4. Melden aan betrokkene

- De CISO (en eventueel het Meldpunt Datalekken) beoordeelt en bepaalt, zonodig in overleg met de FG, aan de hand van de richtlijnen van de Europese Toezichthouders, of er gemeld moet worden aan betrokkene(n).
  De volgende gevallen zijn mogelijk:
  a. Er hoeft niet gemeld te worden aan de betrokkene(n). De motivering wordt opgenomen in het Datalekkenregister.
  b. Er moet gemeld worden aan de betrokken(en).
- Een datalek wordt gemeld aan de betrokkene(n) wanneer de inbreuk een waarschijnlijk hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen.
- Deze melding wordt gedaan in duidelijke en eenvoudige taal. In deze melding wordt minimaal de aard van de inbreuk en de genomen maatregelen gecommuniceerd.
- Een dergelijke kennisgeving is niet noodzakelijk in het geval wanneer er aan één van de volgende voorwaarden is voldaan:
  - Er zijn technische en organisatorische maatregelen genomen om de persoonsgegevens onbegrijpelijk te maken voor onbevoegden en deze maatregelen zijn toegepast op de persoonsgegevens die gelekt zijn;
  - Er zijn achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van de betrokkenen zich niet voordoet;

- Een dergelijke mededeling door de verwerkingsverantwoordelijke zou onevenredige inspanningen vergen. In een dergelijk geval kan men kiezen voor een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

- Indien de betrokkene moet worden geïnformeerd zal de verantwoordelijke lijnmanager dit op zich nemen. Het Meldpunt Datalekken ondersteunt de lijnmanager hierbij.
- Het geniet de voorkeur om betrokkene(n) op individuele basis te benaderen. Bij meer omvangrijke incidenten kan gekozen worden voor algemene voorlichting.

5. Nadere analyse en evaluatie van de melding

- Er wordt door de CISO, het Meldpunt Datalekken en de FG een analyse/evaluatie op de melding uitgevoerd. Het resultaat hiervan wordt vastgelegd in het dossier.
- Zonodig, bijvoorbeeld in het kader van het creëren van bewustwording, koppelt het Meldpunt Datalekken aan de melder terug wat er met zijn melding is gebeurd.

6. Uitvoeren vervolgacties, verbeter- of herstelmaatregelen

- De CISO, het Meldpunt Datalekken en FG onderzoeken of vervolgacties of verbetermaatregelen gewenst zijn.
- Indien het noodzakelijk is om verbetermaatregelen te treffen om het incident op te lossen, worden deze uitgevoerd door de CISO en de verantwoordelijke lijnmanager.
- De CISO ziet erop toe dat de verbetermaatregelen structureel worden geborgd door het ministerie.

7. Sluiting van de melding

- Wanneer de verbetermaatregelen zijn geïmplementeerd of indien er geen vervolgactie noodzakelijk is, sluit de Privacy Officer de melding af.
- De Privacy Officer werkt tot slot het dossier bij.
- De registratie wordt tenminste 3 jaar (*pm check selectielijst*) bewaard ten behoeve van rapportage en verantwoording.

Bijlage 3: Werkinstructie meldplicht datalekken Belastingdienst

Inleiding
Deze werkinstructie beschrijft hoe te handelen en welke stappen moeten worden genomen binnen de Belastingdienst indien er sprake is van een datalek of wanneer een datalek vermoed wordt.

Governance
De minister is de verwerkingsverantwoordelijke voor alle verwerkingen die onder zijn verantwoordelijkheid worden uitgevoerd, dus ook voor verwerkingen door de Belastingdienst. De directeur-generaal Belastingdienst is gemandateerd om gegevensverwerkingen namens de minister uit te voeren en is daarom gemandateerd verwerkingsverantwoordelijke. Het lijnmanagement is verantwoordelijk voor de naleving van privacy en bescherming van de persoonsgegevens binnen de afdeling.

De Belastingdienst heeft een Melddesk Datalekken Belastingdienst (MDB) ingericht voor het beoordelen en afhandelen van incidenten met persoonsgegevens in het kader van de AVG en de WPG.

Voor het in beeld krijgen van deze incidenten is aansluiting gezocht bij het bestaande incidentmanagement van de Belastingdienst onder verantwoordelijkheid van de directie Informatievoorziening (IV).

Hierna volgt de werkinstructie meldplicht datalekken voor de Belastingdienst. De instructie kent de volgende stappen.

1. Signaleren mogelijk datalek
2. Registeren mogelijk datalek
3. Melden aan de Autoriteit Persoonsgegevens (AP)
4. Melden aan betrokkene(n)
5. Nadere analyse en evaluatie van de melding
6. Uitvoeren vervolgacties, verbeter- of herstelmaatregelen
7. Sluiting van de melding

<u>Ad 1 Signaleren mogelijk datalek</u>

- Ieder die kennisneemt van een incident waarbij een inbreuk ten aanzien van persoonsgegevens kan zijn ontstaan, moet hiervan onverwijld melding doen bij de helpdesk [redacted] of aan de postbus Melddesk_Datalekken_Belastingdienst ([redacted]). De meldingen met persoonsgegevens worden door de helpdesk doorgeleid aan en beoordeeld door de Melddesk Datalekken Belastingdienst (MDB).
- De volgende meldingen moeten in ieder geval worden gedaan.
  - Een inbreuk op het netwerk of de bestanden van de Belastingdienst;
  - het ontvangen van een zogenoemde responsible disclosure-melding (melding over een zwakke plek in een ICT-systeem);
  - het verzenden of geven van documenten met persoonsgegevens aan een onjuist persoon;
  - het verliezen of door diefstal vermissen van een gegevensdrager of dossier met daarin e-mails, persoonsgegevens van collega's of persoonsgegevens van belastingplichtigen;

- het verliezen of door diefstal vermissen van een laptop, telefoon of ander device;
- persoonsgegevens die zonder doelbinding in portals ter beschikking gesteld worden of ingezien kunnen worden.

In twijfelgevallen dient men contact op te nemen met de melddesk.

- Een medewerker meldt een potentieel datalek ook bij zijn/haar leidinggevende en directeur. MDB controleert of dit gebeurd is.
- Meldingen van burgers, die een inbreuk met persoonsgegevens melden, of een incident waarbij mogelijk sprake is van een inbreuk, komen bij de Belastingdienst binnen via dienstonderdeel Klanteninteractie&services (KI&S) en worden doorgeleid naar de MDB. Meldingen of vragen over mogelijke inbreuk, bijvoorbeeld van verwerkers, kunnen ook rechtstreeks naar de postbus van de MDB in Lotus Notes worden verzonden via het mailadres: [redacted] of telefonisch via [redacted]
- Indien de Belastingdienst verwerker is, meldt de Belastingdienst het datalek bij zowel de verwerkingsverantwoordelijke als bij het eigen meldpunt. De melding wordt ook opgenomen in het Datalekkenregister van de Belastingdienst. De verwerkingsverantwoordelijke wordt verzocht de informatie over de beoordeling en afhandeling van de melding te communiceren met de Belastingdienst.
- Correspondentie over meldingen of vragen over eventuele inbreuken met persoonsgegevens worden bij voorkeur gericht aan de postbus [redacted] of (indien nodig)

<u>Ad 2 Registreren mogelijk datalek</u>

Meldingen die via de postbus of telefonisch zijn ontvangen worden geregistreerd en ontvangen een uniek nummer in het IT-servicemanagement (ITSM)-systeem en worden (in kopie) aan de MDB verstrekt. Op deze wijze zijn meldingen tevens gekoppeld aan incidenten die worden beoordeeld door de MDB, ook al is de oplossing voor het incident zelf bij een ander team of dienstonderdeel belegd. Op werkdagen wordt door de MDB om 10:00 uur en 14:00 uur een query gedaan op de meldingen van 888. Deze meldingen worden vervolgens ook geregistreerd. De meldingen worden in het systeem klaargezet voor een weging/classificatie door een behandelaar. De stand van zaken over een inbreuk, de wijze van afhandeling en overige vastleggingen vinden plaats in Excel (onder meer voor gebruik in de rapportages). Alle correspondentie wordt in de database in Lotus Notes opgeslagen.

registratie

- In de registratie worden minimaal de volgende gegevens opgenomen.
  - Aard van de inbreuk;
  - De datum en het tijdstip van het datalek of het incident en van het moment van de ontdekking van het datalek;
  - De verantwoordelijke van de desbetreffende verwerking;
  - Contactpersonen van de inbreuk;
  - Omschrijving van de gelekte gegevensset (of een inschatting hiervan);
  - Een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
  - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om deze gevolgen te verhelpen;
  - De maatregelen die de verwerkingsverantwoordelijke heeft getroffen om dergelijke incidenten in de toekomst te voorkomen;

- Een samenvatting van de eventuele communicatie met de toezichthoudende autoriteit en de betrokkene(n);
- Datum en tijdstip van de melding aan de toezichthoudende autoriteit en betrokkene, indien verplicht.

Deze vragen worden beantwoord in het registratieformulier datalek, dat aan de contactpersoon verstrekt wordt door de MDB (tevens vindbaar op intranet

- De administratie neemt meldingen van inbreuken, voor zover nog niet aanwezig, op in ITSM en in de Excel-voortgangsadministratie. De administratie zorgt dat meldingen worden klaargezet voor behandeling. Dit gebeurt minstens twee keer per dag. ITSM, het wegingsformulier, de vastleggingen in Excel en in Lotus Notes vormen samen de datalekregistratie.
- De administratie controleert als een melding is verwerkt of alle stukken opgenomen zijn in Lotus Notes en de melding correct is verwerkt in Excel.
- Een medewerker informatiebeveiliging van de MDB pakt de klaargezette melding op en beoordeelt aan de hand van de beleidsregels van de AP en een wegingslijst of er bij het incident sprake is van een inbreuk met persoonsgegevens. Zijn er geen persoonsgegevens betrokken, dan wordt dit aangetekend in ITSM en wordt het incident gesloten.
- Indien persoonsgegevens zijn betrokken en verwacht wordt dat het een meldingswaardig datalek betreft, wordt een wegingsformulier opgemaakt. Dit wordt door de medewerker voorgelegd aan een collega voor een tweede toetsing of aan de adviseur van de MDB als hij verwacht dat de melding grote impact kan hebben voor betrokkene(n) of de Belastingdienst.
- De MDB registreert de ontvangen en behandelde incidenten per dienstonderdeel en per inbreuksoort zoals deze worden uitgevraagd door de Autoriteit Persoonsgegevens. De rapportage is opgenomen in de rapportage van de Belastingdienst.
- De registratie van de behandelde incidenten bij de MDB, de uitkomst van de weging en de vastlegging van de op grond van het incident genomen correctie- en/of herstelmaatregelen worden drie jaar bewaard voor rapportage en verantwoording en voor evaluatie en communicatie over datalekken.

weging

- Alle meldingen van (mogelijke) inbreuken met persoonsgegevens die binnenkomen bij de MDB worden beoordeeld op inbreuken met persoonsgegevens. Zonodig worden aanvullende vragen gesteld aan de melder of gegevens opgevraagd over het proces. Op basis daarvan wordt een weging gemaakt aan de hand van een stappenplan op basis van de beleidsregels van de Autoriteit Persoonsgegevens. Wegingen met hoge impact voor de betrokkenen of voor de organisatie worden besproken met de privacyofficer, CISO en waar nodig de FG.
- In voorkomende gevallen kan MDB de privacyofficer en/of de CISO consulteren over een mogelijke melding. De privacyofficer en/of de CISO betrekken zonodig de Functionaris voor Gegevensbescherming (FG).
- Meldingsplicht bij de AP en eventueel bericht aan betrokkene(n) wordt beoordeeld aan de hand van het 'mogelijk inhouden van een risico op rechten en vrijheden van de betrokkene' conform de richtlijnen uitgegeven door de AP.
- Het melden van een datalek bij verwerkingen van persoonsgegevens aan de AP en/of de betrokkenen gebeurt uitsluitend door of namens de CIO, zonodig in samenwerking met de FG. Medewerkers melden een datalek niet zelf bij de AP of betrokkene.

- MDB beoordeelt en bepaalt of er sprake is van een meldingsplichtig datalek. De volgende gevallen zijn mogelijk:
    a. Er is geen inbreuk in de zin van de AVG (AVG is niet van toepassing of past niet binnen de definitie van een inbreuk) danwel WPG. Het betreft geen datalek en er wordt niet gemeld aan de AP. De motivering wordt opgenomen in het Datalekkenregister. De melding wordt verder afgehandeld via het gangbare incidentmanagementproces.
    b. Er is wel een inbreuk in de zin van de AVG danwel WPG en het beveiligingsincident wordt geclassificeerd als een datalek.
- Een meldingsplichtig datalek is een situatie waarbij:
    - de AVG of de WPG van toepassing moet zijn;
    - zich daadwerkelijk een (beveiligings)incident heeft voorgedaan. Er is geen meldingsplicht als er nog sprake is van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een inbreuk;
    - persoonsgegevens door verlies of ongeoorloofde verstrekking of door ongeoorloofde toegang onversleuteld in onbevoegde handen zijn gekomen.
- Een meldingsplichtig datalek wordt, gedocumenteerd met de weging, gecommuniceerd aan de directeur van het dienstonderdeel dat betrokken is bij het proces waar het datalek is ontstaan of waar deze impact heeft op de klantbehandeling.
- Naast de directeur worden ook de contactpersoon, de datacoördinator van het dienstonderdeel, de CISO en de privacyofficer geïnformeerd over de melding.
- In deze mededeling wordt aangegeven dat als de melding aan de AP niet compleet kan worden afgedaan (doordat bijvoorbeeld het onderzoek nog niet is afgerond), een vervolgmelding nodig is.
- De contactpersoon wordt geacht de melding zonodig in zijn dienstonderdeel verder te communiceren.
- Wanneer het datalek mogelijk kan leiden tot een risico voor de rechten en vrijheden van natuurlijke personen moet er ook aan betrokkene(n) worden gemeld (zie stap 4). Bij de melding aan de directeur wordt dit aangegeven.
- Wanneer een (mogelijk) datalek naar inschatting van het MDB het karakter heeft van een crisis of een calamiteit wordt, na raadpleging van de privacyofficer en/of de FG, de directie Bureau Bestuursondersteuning en Advies (BBOA) geïnformeerd en persvoorlichting, DG en bewindspersonen. BBOA voert de crisiscoördinatie uit voor het departement;

<u>Ad 3 Melden aan de Autoriteit Persoonsgegevens (AP)</u>

- Een meldingsplichtig datalek moet zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur na het bekend worden bij de dienst worden gemeld bij de AP. Bij het registreren van een (interne of externe) melding start dus een periode van 72 uur waarin alle stappen moeten worden doorlopen.
- De melding wordt gedaan door de MDB. De beoordeling doet het MDB namens de CIO. De privacyofficer, FG en CISO worden geïnformeerd. Indien zich er een risico voordoet, worden de privacyofficer, CISO, FG, CIO, ambtelijke top en bewindspersonen geinformeerd (zie stap 2).
- Een melding kan achteraf worden gewijzigd, aangevuld of ingetrokken als blijkt dat de onderzoeksperiode te kort is geweest om alle relevante weeggegevens beschikbaar te hebben in de beperkte tijd.
- Een inbreuk wordt binnen deze 72 uur, al dan niet voorzien van voldoende gegevens, gemeld door de MDB via de website van de AP. Als er voldoende

gegevens zijn om de melding af te doen wordt deze meteen als volledig gemeld. Zonodig wordt aan de AP aangegeven dat de melding nog niet volledig is onderzocht en dat nadere gegevens volgen in een vervolgmelding.
De ontvangstbevestiging van de melding wordt door de MDB gearchiveerd in het dossier.

Ad 4 Melden aan betrokkene

- Wanneer het datalek mogelijk kan leiden tot een risico voor de rechten en vrijheden van natuurlijke personen, moet er ook aan betrokkene(n) worden gemeld. Een datalek kan immers voor betrokkene(n) grote gevolgen hebben, waaronder verlies van controle over hun persoonsgegevens inclusief financiële positie, beperking van hun rechten, discriminatie, identiteitsdiefstal en mogelijke financiële verliezen.
  Bij de melding aan de directeur wordt dit aangegeven. De directeur organiseert vervolgens mededeling aan betrokkene(n), hierbij ondersteund door de datacoördinator.
- Deze melding wordt gedaan in duidelijke en eenvoudige taal. In deze melding worden minimaal de aard van de inbreuk en de genomen maatregelen gecommuniceerd. De MDB heeft hiervoor een voorbeeldtekst beschikbaar. De MDB adviseert het dienstonderdeel indien gewenst over de inhoud van bericht.
- De MDB en de privacy-officer ontvangen een afschrift van dit bericht. De MDB voegt een afschrift van het bericht aan betrokkenen toe aan haar dossier.
- Een dergelijke kennisgeving is niet noodzakelijk in het geval wanneer er aan één van de volgende voorwaarden is voldaan:
  - Er zijn technische en organisatorische maatregelen genomen om de persoonsgegevens onbegrijpelijk te maken voor onbevoegden en deze maatregelen zijn toegepast op de persoonsgegevens die gelekt zijn;
  - Er zijn achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van de betrokkenen zich niet voordoet;
  - Een dergelijke mededeling door de verwerkingsverantwoordelijke zou onevenredige inspanningen vergen. In een dergelijk geval kan men kiezen voor een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.
  - Er zijn zwaarwegende redenen om de betrokkene niet te informeren, bijvoorbeeld als er een (strafrechtelijk of fiscaal) onderzoek loopt.
  - Indien de gegevens vallen onder de Wet Politiegegevens kan de mededeling aan de betrokkene worden uitgesteld, beperkt of achterwege gelaten:
    - ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
    - ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
    - ter bescherming van de openbare veiligheid;
    - ter bescherming van de rechten en vrijheden van derden;
    - ter bescherming van de nationale veiligheid.

  De verantwoordelijke binnen het dienstonderdeel dat onder de WPG werkt, maakt deze afweging en informeert de MDB. De MDB registreert dit.
- Het geniet de voorkeur om betrokkene(n) op individuele basis te benaderen. Bij meer omvangrijke incidenten kan gekozen worden voor algemene voorlichting.
- In geval een datalek is behandeld waarbij beoordeeld is dat geen bericht aan betrokkene nodig is, wordt deze ten minste een keer herbeoordeeld. Dit zal op 3

momenten per jaar bij een analyse plaatsvinden. Mocht alsnog bericht aan betrokkenen noodzakelijk zijn, dan wordt dit in gang gezet.

Ad 5 Nadere analyse en evaluatie van de melding

- Als er een incident plaatsvindt, dan analyseert het dienstonderdeel waar het incident is ontstaan de oorzaak en zal waar mogelijk maatregelen treffen ter voorkoming van herhaling.

Ad 6 Uitvoeren vervolgacties, verbeter- of herstelmaatregelen

- Het dienstonderdeel, verantwoordelijk voor het proces waar de inbreuk is ontstaan, neemt ten aanzien van de inbreuk herstelmaatregelen en neemt waar nodig corrigerende maatregelen voor het proces waar de inbreuk is ontstaan. Deze maatregelen worden meegedeeld aan de MDB, die hiervan de verplichte registratie voert. De data-coördinator meldt waar nodig de voortgang aan de directeur.
- De MDB vraagt de door de Belastingdienst genomen herstelmaatregel(en) en mogelijke correctieve maatregelen aan de MDB bekend te maken om deze vast te leggen in het dossier.
- MDB beoordeelt periodiek (ten minste 3 keer per jaar) of er meldingen met een repeterend karakter zijn en neemt contact met de CISO en proceseigenaar of ketenmanager over mogelijke correctiemaatregelen of aanpassingen in het proces. De MDB legt dit vast in het dossier.
- De CISO betrekt deze informatie bij de analyses over de issues en dieperliggende oorzaken daarvan op het gebied van informatiebeveiliging als onderdeel van de pdca-cyclus. De CISO (en zonodig de privacyofficer en de FG) onderzoekt op basis van trends en rapportages Belastingdienst-breed de effectiviteit van de geïmplementeerde maatregelen.
- Indien het noodzakelijk is om verbetermaatregelen te treffen worden deze uitgevoerd door de verantwoordelijke lijnmanager, waar nodig geadviseerd door de eigen informatiebeveiligings-functionaris en/of de CISO. De CISO stelt zonodig vast dat bestaande kaders niet voldoen, past de kaders in dat geval aan, en stelt vast of er aanvullend/aangepast beleid nodig is om het incident in de toekomst te voorkomen.
- De CISO ziet erop toe dat de verbetermaatregelen structureel worden geborgd door de lijnmanager.
- Er vindt terugkoppeling plaats naar de dienstonderdelen via de maandelijkse rapportages.

Ad 7 Sluiting van de melding

- Wanneer de verbetermaatregelen zijn geïmplementeerd of indien er geen vervolgactie noodzakelijk is, sluit de MDB de melding af.
- De registratie wordt 3 jaar bewaard ten behoeve van rapportage en verantwoording.

Verantwoord omgaan met gegevens

Publicatiedatum 08-06-2020, 16:16 | Laatste update 18-12-2020, 11:59

Of je nu werkt in de handhaving, opsporing, ICT of administratieve processen: in jouw werk heb je te maken met gegevens en vertrouwelijke informatie. Zoals persoonsgegevens, fiscale gegevens, maar ook beleidsstukken en plannen. Deze zijn van onschatbare waarde. Enerzijds om onze dienstverlening te verbeteren, bijvoorbeeld met vooraf ingevulde aangiftes. Anderzijds om de handhaving, het toezicht en de opsporing rechtvaardig en effectief uit te voeren.

Het werk bij de Belastingdienst kenmerkt zich onder meer, door de aanwezigheid van veel waardevolle (voor)kennis en gegevens over:

- burgers en bedrijven, zoals privacygevoelige (persoons)gegevens
- de wijziging van regelgeving, zoals financiële wetgeving en komende fiscale maatregelen
- en onze processen, zoals de uitvoering en fiscale controles van maatregelen

Des te meer reden om hier verantwoord mee om te gaan.

Wist je dat?

De Belastingdienst heeft de grootste gegevensverzameling binnen de overheid. Wij:

- ontvangen gegevens van burgers en bedrijven
- winnen gegevens in bij veel (overheids)organisaties
- verstrekken gegevens aan andere overheidsinstanties

Elke aanslag of andere beslissing is gebaseerd op de gegevens in onze systemen; deze moeten dus altijd correct en up-to-date zijn. Daarnaast mogen gegevens alleen beschikbaar zijn voor wie dat nodig heeft voor het werk. Daarom is het cruciaal dat we bewust, veilig en vertrouwelijk omgaan met deze gegevens. Jij als medewerker en de Belastingdienst als organisatie.

Hoe ga jij om met gegevens?

Bij het tijd-, plaats- en apparaatonafhankelijk werken, wil je gegevens gemakkelijk kunnen benaderen en delen. Dit brengt risico's met zich mee. Door digitaal veilig te werken, help je voorkomen dat onbevoegden toegang krijgen tot de gegevens. Hieronder vind je een overzicht met algemene gedragsregels. Wellicht gelden voor jouw werk ruimere of juist minder ruime regels. Kijk daarvoor op de pagina van jouw onderdeel of vraag je leidinggevende.

Verplichte opleiding

Alle medewerkers zijn verplicht de e-learning module iBewustzijn en de module AVG te volgen. Heb je dit nog niet gedaan, volg ze dan bij de BelastingdienstAcademie:

2. Ga naar Mijn leeromgeving.
3. Vul in het zoekvenster de term:
   - iBewustzijn in om bij de module 'Hoe veilig en bewust omgaan met gegevens' te komen.
   - AVG in om bij de module AVG te komen.
4. Sla de certificaten op in P-Direkt.

De module iBewustzijn bestaat uit 4 delen. Voor elk deel krijg je een certificaat. Het is de bedoeling dat je dit certificaat in P-Direkt opslaat zodat je kunt aantonen dat je de cursus hebt gehaald.

Toegang tot de systemen

Het primaire proces wordt ondersteund door systemen. Deze systemen bevatten de gegevens die de Belastingdienst nodig heeft voor het uitvoeren van haar taak. Deze systemen worden zowel technisch als organisatorisch beveiligd tegen toegang door onbevoegden. Autorisaties zorgen ervoor dat medewerkers alleen bij die gegevens kunnen die zij nodig hebben voor hun werk.

- Aanvragen en wijzigen van autorisaties.
- Kies een veilig wachtwoord en houd het voor jezelf.

Tip: Er is een handig hulpmiddel beschikbaar voor het veilig onthouden van wachtwoorden: Keepass.

Gebruik van DWB, tablet en smartphone

Deze apparaten zorgen ervoor dat je de gegevens op de systemen kan benaderen. Ze geven daarnaast ook toegang tot andere applicaties en het internet Ga verantwoord om met je apparaten:

- Installeer de apparaten volgens de instructie die je hebt gekregen bij het apparaat.
- Installeer updates zodra ze beschikbaar zijn.
- Beperk privégebruik.
- Laat andere personen jouw account niet gebruiken.
- Gebruik alleen externe gegevensdragers, zoals USB-sticks, wanneer je daarvoor geautoriseerd bent.

Installeren van apps

- Ga na welke toegangsrechten een app vraagt. Wees kritisch in wat je toestaat.
- Op je zakelijke mobiele apparaat vind je in app "Apps@Work" goedgekeurde apps.

Wees bewust van de omgeving

Of je nu op je werkplek, thuis, in de trein of in een openbare ruimte bent, voorkom altijd dat anderen kunnen meekijken op je scherm of in je papieren.

- Ruim documenten en aantekeningen op en maak whiteboards schoon na gebruik.
- Wees bewust wie kunnen meeluisteren naar je gesprek of presentatie.
- Gebruik een privacyscherm om kans op meekijken te verkleinen. Vraag je teamleider naar de mogelijkheden.
- Laat apparaten niet onbeheerd achter, ook niet in een afgesloten auto.
- Vergrendel je DWB wanneer je deze niet gebruikt: Dit kan op 2 manieren:
- Windowslogo + L ,of via
- Ctrl+Alt+Delete en dan optie: Vergrendelen

Op de werkplek
Binnen de gebouwen van de Belastingdienst rekenen medewerkers erop dat er geen onbevoegden zijn.

- Meld je bezoekers aan en begeleid ze tijdens het gehele bezoek.
- Draag je toegangspas zichtbaar zodat duidelijk is dat jij een collega bent.

Buitenland
In principe neem je geen apparaten mee naar het buitenland. Wordt dit wel gevraagd door jouw leidinggevende, houd dan rekening met extra risico's die staan op de pagina 'Internetgebruik Belastingdienst'.

Voorkom online criminaliteit

Jouw apparaten zijn verbonden met het internet. Ook als je het niet verwacht. Zo slaan apps jouw gegevens misschien wel op, op een plek waar je dat niet verwacht. Wat kun je doen om te voorkomen dat er bewust misbruik wordt gemaakt van jouw accounts of apparaten?

- Als je een openbaar netwerk niet vertrouwt, kun je de hotspotfunctie van je zakelijke smartphone gebruiken. Meer over internetgebruik bij de Belastingdienst.
- Gebruik voor ieder account een uniek wachtwoord. Tip: Keepass is een handig hulpmiddel voor het veilig bewaren van jouw wachtwoorden.
- Klik alleen op links, pop-ups of banners als je deze vertrouwt. Controleer of een email, site of link wel een adres heeft dat je kent of kunt verwachten. Tip: door met de muisaanwijzer op een link te staan, zonder te klikken, zie je het webadres waar je naartoe geleid wordt. Controleer dit. Bij mobiele apparatenmoet je de link wat langer ingedrukt houden.
- Wees bij e-mails van (schijnbare) bekende afzenders alert op ongebruikelijke vragen of op de vraag naar persoonsgegevens.
- Vul alleen inloggegevens in als je de herkomst van de site hebt gecontroleerd
- Verloopt de inlogprocedure anders dan normaal? Neem dan direct contact op met de Servicedesk-ICT.

Verwerken van persoonsgegevens of vertrouwelijke informatie

Naast het gebruik van gegevens uit de systemen maak je in je werk ook gebruik van documenten en bestanden. Deze kunnen persoonsgegevens of vertrouwelijke informatie bevatten. Waar houd je rekening mee?

Verwerk je persoonsgegevens?
Een verwerking van persoonsgegevens is bijvoorbeeld het ontvangen, verzamelen, raadplegen, versturen en analyseren ervan. Als bijvoorbeeld het document waarmee je werkt persoonsgegevens bevat, ga dan na of je deze verwerkt conform de eisen die de Algemene verordening gegevensbescherming (AVG) hieraan stelt. Van belang zijn onder meer vragen als:

- Zijn de persoonsgegevens wel verzameld voor het doel waarvoor je ze nu wil gebruiken?
- Kan je ook met minder persoonsgegevens toe (dataminimalisatie)?
- Is pseudonimisering of anonimisering mogelijk? Dus het vervangen van de persoonsgegevens door andere gegevens die niet direct herleidbaar zijn tot persoonsgegevens.

Denk ook goed na over de grondslag (de reden waarom).

Wanneer je persoonsgegevens gaat verzamelen of verwerken voor een (nieuw) bestand, document of proces, neem dan altijd contact op met jouw teamleider of datacoördinator.

Persoonsgegevens van medewerkers
De AVG maakt geen onderscheid in gebruik van persoonsgegevens van burgers en medewerkers. Heb jij in je werk te maken met persoonsgegevens van medewerkers bij de Belastingdienst? Houd dan rekening met dezelfde regels als hierboven. De grondslag 'toestemming van persoon om wie het gaat' zal intern vrijwel niet gebruikt worden.

Opsporing
Medewerkers in de opsporing hebben te maken met de Wet politiegegevens (WPG) die aangeeft hoe zij met gegevens omgaan.

Opslaan, archiveren en delen documenten en berichten

Je wilt bestanden of berichten natuurlijk opslaan of delen. Ook hierin staan wellicht persoonsgegevens of vertrouwelijke informatie. Waar houd je rekening mee?

Opslaan van documenten en berichten

- Sla bestanden alleen op in de systemen en de samenwerkingsgebieden van de Belastingdienst. Dat betekent ook dat je geen documenten naar je privé e-mail stuurt.
- Gebruik geen app die bestanden opslaat op externe plaatsen (in de cloud) of waarvan je niet weet waar de gegevens opgeslagen worden.

Delen van bestanden en berichten

- Bepaal wie er bij je bestanden mag door ze op de juiste plek of community te zetten.
- Realiseer je dat je niet altijd weet wie er meekijkt bij gebruik van chat- of vergaderprogramma's, zoals Webex.
- Moet je voor je werk grote bestanden delen met externe partijen gebruik dan Belastingdienst filetransfer.

Archiveren, schonen en vernietigen van je documenten

- Documenten die een relatie hebben met het uitvoeren van je taken, moeten door jou worden gearchiveerd. Gebruik voor het archiveren van fysieke documenten het aanbiedingsformulier.
- Volg voor het archiveren en het opschonen van documenten uit je digitale werkomgeving de informatiebladen op de community 'Archiveren en Vernietigen'.
- Sommige documenten worden blijvend bewaard, andere documenten moeten op termijn worden vernietigd. In selectielijsten is voor alle werkprocessen vastgesteld wat de vernietigingstermijnen zijn. Bij vernietiging uit je digitale werkomgeving moet je de vernietigingsprocedure volgen en een verklaring opstellen.

Als het misgaat

Iedereen doet zijn best verantwoord om te gaan met gegevens. Toch gaat het weleens mis. Dit kun jij doen als het misgaat.

Incidenten met persoonsgegevens moet je melden
Alle incidenten met persoonsgegevens moeten bij de Melddesk datalekken worden gemeld. Bij Douane gebruik je de app 'Bijzondere voorvallen'. Voorbeelden van incidenten zijn: het lekken van persoonsgegevens door bijvoorbeeld dossiers of gegevensdragers te verliezen zoals laptops, smartphones en tablets. Maar ook door het versturen van gegevens aan onjuiste (e-mail)adressen.

Kortom, situaties waarin wordt afgeweken van de privacywetgeving moet je zo snel mogelijk melden bij de melddesk datalekken en voor Douane op de app 'bijzondere voorvallen'. Zij bepalen vervolgens of het daadwerkelijk om een datalek gaat en hoe de verdere afhandeling eruit ziet.

Schade, verlies of diefstal
Bij schade, verlies of diefstal van mobiele apparatenwerkplekken of randapparatuur moet je een melding beveiligingsincident opmaken. Doe dit samen met je leidinggevende.

Virus
Verdachte mail ontvangen? Verwijder deze niet. Neem contact op met de ICT-Servicedesk. Informeer de ICT-Servicedesk en je collega's als je DWB-laptop besmet is met een virus of wanneer er een verdachte e-mail in omloop is.

Phishing
Bij phishing verander je onmiddellijk het wachtwoord. Gebruik je toch nog het wachtwoord op andere accounts? Verander deze dan ook. Phishing is oplichting door mensen te lokken naar een valse omgeving en ze daar nietsvermoedend gegevens te laten invullen, zoals inlognaam, en wachtwoord. Verdachte phishing mail ontvangen? Verwijder deze niet. Neem contact op met de ICT-Servicedesk.

Waar kan ik terecht met vragen?

Datacoördinator
Binnen iedere directie zijn de taken en verantwoordelijkheden met betrekking tot privacyvraagstukken formeel belegd binnen het management. Het management wordt daarbij ondersteund door de datacoördinatoren en / of privacyfunctionarissen (Wpg) . Deze medewerkers zijn, naast jouw teamleider, jouw eerste aanspreekpunt met betrekking tot privacy vraagstukken. Overzicht datacoördinatoren.

Vaktechnisch Aanspreekpunt (VTA) en Vaktechnisch Coördinator (VACO) Formeel recht
De VTA's en VACO's staan dichtbij de medewerkers in de teams. Zij fungeren als schakel en als vraagbaak over vaktechnische vraagstukken op het snijvlak van uitvoering en beleid. De VTA's en VACO's worden ondersteund door Team Juridisch Advies Gegevens (JAG) van CAP.

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) is de interne privacy-toezichthouder. Deze persoon houdt binnen de Belastingdienst toezicht op de toepassing en naleving van de privacywetgeving

Vertrouwenspersoon integriteit
Als persoonsgegevens moedwillig gelekt worden, dan is er sprake van een integriteitsschending. Je kunt (het vermoeden van) een integriteitsschending of misstand melden bij je leidinggevende maar ook bij de vertrouwenspersonen integriteit of bij de postbus commissieintegriteitbelastingdienst@rijksoverheid.nl.

Hoe gaat de Belastingdienst om met gegevens?

De Belastingdienst heeft wettelijke bevoegdheden en verplichtingen als het gaat om het verkrijgen, verwerken en verstrekken van gegevens. Daarnaast helpt het effectief inzetten van gegevens bij het verbeteren van de dienstverlening aan burgers en bedrijven en het houden van toezicht.

De bescherming van deze gegevens is belangrijk, bij de verschillende aspecten van ons eigen werk én in onze samenwerking met anderen. De Belastingdienst zet daarom steeds stappen om de diverse aspecten van het verkrijgen, verwerken en verstrekken van gegevens verder te verbeteren. Hiervoor zijn de 10 basisprincipes opgesteld.

Dit doen we steeds meer met moderne technieken. Bijvoorbeeld bij het vooraf invullen van zoveel mogelijk gegevens in de online aangifte inkomstenbelasting. En bij het gebruik van data-analyse. Effectief inzetten van gegevens helpt zo bij het goed inrichten van dienstverlening en bij het houden van toezicht. Dit zijn dan ook belangrijke thema's in de Investeringsagenda waarmee de Belastingdienst toekomstbestendig wordt gemaakt. Hoe we dat doen lees je op de pagina Datagedreven werken en sturen is datamodellen samenstellen en vertellen.

Datagedreven werken en sturen is datamodellen samenstellen en vertellen

Door het uitvoeren van de fiscale wetgeving en het uitkeren van toeslagen draagt de Belastingdienst bij aan een financieel gezond Nederland. Data is hierbij onmisbaar, het is de grondstof van al het werk bij de dienst. Lees hier meer over op de pagina Datagedreven werken en sturen is datamodellen samenstellen en vertellen.

Wetgeving

Naast dat we er zelf een groot belang bij hebben om de gegevens op orde te hebben en houden, wordt er vanuit beleid en wetgeving ook eisen gesteld aan hoe wij dat doen.

Tags: avg, gegevens

Inhoudelijke suggesties?

Terug naar boven

Op deze pagina Op deze pagina

- Hoe ga jij om met gegevens?
- Hoe gaat de Belastingdienst om met gegevens?

- Datagedreven werken en sturen

Op deze pagina

- Hoe ga jij om met gegevens?
- Hoe gaat de Belastingdienst om met gegevens?
- Datagedreven werken en sturen
- Terug naar boven

Over deze subsite

- Contact
- Tag index

Over intranet

- Sitemap Intranet
- Over intranet
- Intranet op ConnectPeople
- Privacyverklaring
- Inloggen redacteuren

Veld	regel 2018/136	regel 2018/1460
ITSM nummer	1180224058	1180041184
Gekoppeld ITSM nr.	1180223991	1180040208
Datum incident	17-8-2018	6-2-2018
Datum/tijd melding ontvangen dienst		
Datum/tijd melding ontvangen MDB	17-8-2018 10:15	6-2-2018
Behandeld door	[redacted]	[redacted]
Naam melder	[redacted]	
Dienstonderdeel	IV	GO
Naam contactpersoon		[redacted]
Omschrijving	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.
Proces cf verwerkingenregister		
Aantal betrokkenen		
BSN 1 betrokkene		
Naam 1 betrokkene		
Meldplichtig datalek ja/nee	Ja	Ja
Collegiale tegenlezing Weging		
Datum melding AP	17-8-2018 13:54	9-2-2018 00:00
Uniek nummer melding AP	[redacted]	[redacted]
Melding AP 1/Voorlopig 2/N.v.t. 3/Definitief	3	3
Bericht Betrokk.	Nee	Ja
Check bij DO bericht betrokkene		9-3-2018
Datum verz. bericht betrokk.		Telefonisch geinformeerd
Overige informatie	DWB ontvreemd uit auto met documenten met persoonsgegevens collega's, geen burger gegevens bij betrokken	verlies DWB, ipad en documenten GO

ITSM nummer	1190034064	1190068119	1190111214	1190126543
Gekoppeld ITSM nr.		1190067743		1190126522
Datum incident	5-2-2019	8-3-2019	19-4-2019	8-5-2019
Datum/tijd melding ontvangen dienst	5-2-2019 15:30	8-3-2019 10:21	19-4-2019 12:20	8-5-2019 10:07
Datum/tijd melding ontvangen MDB	6-2-2019 10:43	8-3-2019 14:15	19-4-2019 12:26	8-5-2019 10:15
Behandeld door	[redacted]	[redacted]	[redacted]	[redacted]
Naam melder	[redacted]	[redacted]	[redacted]	[redacted]
Naam contactpersoon	[redacted]	[redacted]	[redacted]	[redacted]
Dienstonderdeel	MKB	Toeslagen	MKB	CAP
Omschrijving	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Device en/of papier met persoonsgegevens kwijtgeraakt of gestolen.
Aantal betrokkenen	2	3	50	19
BSN betrokkene	onbekend	[redacted]	onbekend	Onbekend
Naam 1 betrokkene	onbekend	[redacted]	onbekend	Onbekend
Meldplichtig datalek ja/nee	Ja	Ja	Ja	Ja
Collegiale tegenlezing Weging	[redacted]	[redacted]	[redacted]	[redacted]
Datum melding AP	6-2-2019 16:18	8-3-2019 16:02	19-4-2019 21:07	9-5-2019 14:01
Uniek nummer melding AP	[redacted]	[redacted]	[redacted]	[redacted]
Risico cat				
Melding AP	Definitief	Definitief	Definitief	Ingetrokken
Bericht Betrokk.	Ja	Ja	Ja	N.v.t.
Check bij DO bericht betrokkene	13-2-2019	15-3-2019	26-4-2019	
Datum verzonden bericht betrokk.	11-2-2019	22-3-2019	26-4-2019	
Datum intrekken indien van toepas				10-5-2019
Overige informatie	pril controledossier kwijtgeraakt/gestolen met persoonsgegevens van belastingplichtig en zijn adviseur	dwb gestolen. Op 11 maart toelichting melding ook een fysiek dossier gestolen. Een nadere vervolgmelding gedaan voor het compleet maken van de melding	DWB en fiscaal dossier gestolen tijdens treinreis, Dossier bevat persoonsgegevens, uitgezocht moet worden wie de betrokkenen zijn.	Tas gestolen met stukken, laptop en telefoon. / Tas met inhoud is terug.

ITSM nummer	1200008146	1200008502	1200036523
Gekoppeld ITSM nr.	1200007547		
Datum incident	9-1-2020	10-1-2020	6-2-2020
Datum/tijd melding ontvangen dienst	9-1-2020 18:50	10-1-2020 10:37	7-2-2020 08:03
Datum/tijd melding ontvangen MDB	10-1-2020 10:15	10-1-2020 10:37	7-2-2020 10:01
Behandeld door	[redacted]	[redacted]	[redacted]
Naam melder	[redacted]	[redacted]	[redacted]
Naam contactperson	[redacted]	[redacted]	
Dienstonderdeel	MKB	CAP	MKB
Omschrijving	Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen.	Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen.
Aantal betrokkenen	50	1	18
Meldplichtig datalek ja/nee	Ja	ja	ja
Datum melding AP	10-1-2020 16:59	13-1-2020 12:27	10-2-2020 11:44
Uniek nummer melding AP	[redacted]	[redacted]	[redacted]
Risico cat	1	2	2
Melding AP	Definitief	Definitief	Definitief
Bericht Betrokk.	N.v.t.	Ja	Nee
Check bij DO bericht betrokkene		20-1-2020	
Datum verzonden bericht betrokk.		14-1-2020	
Overige informatie	Dwb uit auto gestolen. Ook 1 dossier, betreft geen info van NP(of herl.baar). Aanvulling: wel namen medew.als behandelaar genoemd. 4 Rechtspers en medew.zijn geinformeerd door TL.	Dossier op bet.aut. parkeergarage laten liggen. Vinder heeft dossier bij rechtbank afgegeven.	Auto inbraak waarbij laptop en dossiers zijn gestolen. Gossiers teruggevonden in de staat zoals ze waren bij het kwijtraken.