Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Directoraat-Generaal
Belastingdienst

Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Inlichtingen

Ons kenmerk
2016-0000172062

Uw brief (kenmerk)
d.d. 12 oktober 2016

Datum 26 oktober 2016
Betreft Wob-verzoek beleid met betrekking tot thuiswerken medewerkers Belastingdienst

Geachte ,

Op 12 oktober 2016 stuurde u mij een Wob-verzoek. In dit verzoek vraagt u mij documenten openbaar te maken die betrekking hebben op 'het thuiswerken van medewerkers van de Belastingdienst met gegevens van burgers en bedrijven op (al dan niet eigen) computers en in systemen van de Belastingdienst.'

Wettelijk kader
Uitgangspunt van de Wob is dat - in het belang van een goede en democratische bestuursvoering - overheidsdocumenten op verzoek openbaar worden gemaakt. Dit uitgangspunt geldt niet als een specifieke geheimhoudingsplicht zich ertegen verzet of als één of meer uitzonderingsgronden van de Wob van toepassing zijn. Het verzoek moet betrekking hebben op documenten die feitelijk beschikbaar zijn en niet al openbaar gemaakt zijn.

Beoordeling van uw verzoek
Medewerkers van de Belastingdienst die toegang moeten hebben tot de systemen van de Belastingdienst om gegevens van belastingplichtigen te kunnen raadplegen en verwerken doen dat altijd met apparatuur die door de Belastingdienst aan hen ter beschikking is gesteld. De autorisatie om thuis te kunnen werken staat standaard uit. Alleen na toestemming van de teammanager kan een medewerker autorisatie krijgen om buiten kantoor werkzaamheden te verrichten waarvoor toegang tot de Belastingdienstsystemen nodig is. Het is niet mogelijk toegang te krijgen tot deze systemen met een privé computer. Uiteraard is de verstrekte apparatuur ook beveiligd volgens de geldende standaarden, zoals het altijd gebruik maken van beveiligde verbindingen.

De Belastingdienst hecht groot belang aan integriteit en beveiliging van informatie. Dat is terug te vinden in diverse documenten die openbaar zijn gemaakt. Recent is een Wob-besluit openbaar gemaakt waarin dit onderwerp ook aan de orde kwam. Gemakshalve verwijs ik daarnaar[1].

[1] https://www.rijksoverheid.nl/documenten/wob-verzoeken/2016/10/19/besluit-wob-verzoek-inzake-disciplinaire-straffen-bij-de-belastingdienst

Directoraat-Generaal
Belastingdienst

Ons kenmerk
2016-0000172062

Op het intranet van de Belastingdienst is één artikel gewijd aan beveiliging van gegevens. Ik maak dit document openbaar. Een afdruk ervan voeg ik als bijlage bij dit besluit.

Besluit
Ik wijs uw verzoek toe.[2]

Hoogachtend,
de staatssecretaris van Financiën,
namens deze,

mr. J de Blieck
lid van het managementteam Belastingdienst

[2] Deze brief 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 moet worden gericht aan de Staatssecretaris van Financiën, kamer KV 2.52, postbus 20201, 2500 EE Den Haag. Het bezwaarschrift moet worden ondertekend en ten minste het volgende bevatten:
a. naam en adres van de indiener;
b. de dagtekening;
c. een omschrijving van het besluit waartegen het bezwaar zich richt;
d. een opgave van de redenen waarom u zich met het besluit niet kunt verenigen.

Belastingdienst

Intranet > Personeel > Integriteit > Regels en procedures > Beveiliging van gegevens

Beveiliging van gegevens

Laatste update: 25 januari 2016

Tags : beveiliging, clean desk, gedragscode internet, gegevens, handboek, integriteit, vertrouwelijke gegevens

Werk veilig en vaardig: wees iBewust

Burgers moeten erop kunnen vertrouwen dat hun gegevens veilig zijn bij de Belastingdienst. Met de beveiligingsmaatregelen worden 80% van de risico's ondervangen. Voor de overige 20% heeft de Belastingdienst de hulp nodig van de medewerkers. Lees hieronder wat jij kunt doen om bewust om te gaan met informatie: binnen, buiten, achter je scherm, in de cloud of op social media.

Binnen het kantoor

De Belastingdienst verwacht van medewerkers dat zij hun rijkspas zichtbaar dragen en hun bezoekers begeleiden. Spreek onbekende personen op jouw afdeling aan.

Gebruik van je Digitale Werkplek Belastingdienst (DWB)

De DWB-werkplek heeft een hoog beveiligingsniveau. Met je DWB-werkplek kun je op een veilige manier remote werken. Vanaf elke plek is namelijk een veilige verbinding opgezet met het Belastingdienstnetwerk. Met die verbinding is de informatie die je verstuurt, volledig afgeschermd.

Werk je met vertrouwelijke gegevens op je DWB, dan is het belangrijk dat alleen jij die gegevens kan inzien. Schakel daarom altijd je schermbeveiliging in als je je werkplek verlaat, en berg dossiers en elektronische gegevensdragers op. Wachtwoorden mag je aan niemand geven, ook niet aan je naaste collega's. Natuurlijk geldt dit allemaal ook voor mobiele devices zoals tablet en smartphone.

E-mail en internet

De Belastingdienst biedt e-mail en internet op de werkplek aan als bedrijfsmiddel, bedoeld voor zakelijk gebruik bij de uitvoering van de werkzaamheden. Medewerkers mogen internet en e-mail incidenteel en kortstondig voor privédoeleinden gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het gebruik een redelijk doel dient. Alle informatie over wat wel en niet is toegestaan bij mailen, vind je in de handleiding over Extern mailen.

Ga voorzichtig om met verdachte e-mails, bestanden en inlogschermen op internetsites:

- geef nooit inloggegevens of vertrouwelijke informatie
- check de website waar je inlogt
- let op verdachte internetsites. Check waar een verkorte link naartoe verwijst door deze te plakken op de speciale site longurl.org. Longurl.org toont je vervolgens de volledige url zodat je kunt beoordelen of dit de site is die je verwachtte

- installeer zelf geen software

Mobiele apparaten

Met Mobile@Work wordt de beveiliging van onze zakelijke informatie op mobiele toestellen verbeterd en toegang tot diensten binnen het Belastingdienstnetwerk eenduidig en eenvoudig geregeld. Het wordt mogelijk om (de apps op) de mobiele toestellen te beheren en op afstand te configureren. Je vindt meer over Mobile@Work in de community "Toegang Mobiele Diensten (Mobile@Work)".

Op mobiele apparaten zoals smartphones en tablets is de installatie van Mobiele mail verplicht. Hiermee kan de Belastingdienst op afstand data op mobiele apparaten wissen. Mobiele mail zorgt er ook voor dat de maildata in een veilige 'container' wordt opgeslagen. Bovendien stel je bij Mobiele mail een pincode in op jouw mobiele toestel. Bij 10 verkeerd ingetoetste pincodes wordt alle data op het apparaat gewist. Wat kan je zelf doen?

- gebruik een onvoorspelbare pincode
- wijzig je pincode regelmatig
- beveilig en versleutel je data extra met de Goodreader app. Het versleutelen van data is essentieel op mobiele apparaten omdat computers deze apparaten vaak herkennen als USB device
- sla geen zakelijke data op in een publieke cloud (bijvoorbeeld iCloud, Hotmail, Skydrive, Google Docs etc.) maar gebruik hiervoor de Belastingdienstcloud: ConnectPeople. De data staat dan veilig in het datacenter van de Belastingdienst.

Wat te doen bij een virus, verlies en diefstal

Mocht je een virus hebben of je apparaat onverhoopt kwijtraken, neem dan altijd direct contact op met de B/CIE Servicedesk (555 of 088 - 1568 555). Zij kunnen jouw apparaat op afstand wissen.

Bij verlies of diefstal moet je daarnaast aangifte doen bij de politie en dit melden aan je leidinggevende.

Sociale media en online communicatie

Het gebruik van sociale media wordt voor ons werk steeds belangrijker. Hoe ga je hier nu goed mee om en waar ligt de grens tussen werk en privé? Het gebruik van sociale media is gebonden aan bepaalde regels. Net als bij andere soorten van communicatie houd je in je uitingen via sociale media rekening met de basiswaarden van de Belastingdienst. Bedenk daarbij dat wat je op internet plaatst lange tijd beschikbaar blijft en makkelijk door anderen kan worden gebruikt, misbruikt of verkeerd geïnterpreteerd.

Voorkom onbewust lekken, verkeerde interpretaties of imagoschade:

- wees zorgvuldig, zakelijk, betrouwbaar, constructief en respectvol
- lees je bijdrage vóór verzending nog eens na of laat deze een paar uur in concept staan. Dit kan in veel gevallen een hoop ellende voorkomen
- communiceer niet over zaken die nu of in de toekomst schadelijk kunnen zijn voor de Belastingdienst, je collega's, belastingplichtigen of andere belanghebbenden. Dit kan betrekking hebben op teksten, citaten, foto's en/of filmpjes die je plaatst

Bekijk ook de uitgangspunten voor online communicatie voor rijksambtenaren.

Voorkom misbruik en virusverspreiding:

- beperk toegang tot je profiel alleen tot vrienden en bekenden
- accepteer uitsluitend uitnodigingen van bekenden. Twijfel je aan de echtheid van een boodschap, neem dan via e-mail of telefoon contact op met die persoon om de boodschap te verifiëren

- gebruik sterke wachtwoorden zodat je inloggegevens moeilijker achterhaald kunnen worden
- zorg ervoor dat je virusscanner, software en browser up to date zijn