Ministerie van Financiën

notitie

Eisen Internetplekken voor digitaal zaken doen met de Belastingdienst bij de bibliotheken

Aanleiding

Op 18 februari 2016 hebben de Belastingdienst en de Koninklijke Bibliotheek (KB) een convenant ondertekend. Dit legt de samenwerking vast tussen de KB en de Belastingdienst bij het ondersteunen van burgers bij het digitaal zaken doen met de overheid. In dit convenant is onder meer afgesproken dat vanaf najaar 2016 er gratis toegang tot computers met internet- en printfaciliteiten bij circa 800 vestigingen van lokale bibliotheken beschikbaar zal zijn, om zaken met de overheid in het algemeen en de Belastingdienst in het bijzonder te regelen.

Concreet betekent dat dat de Belastingdienst burgers die niet zelf over een computer of internetverbinding beschikken en ver van een Belastingdienstbalie wonen, kunnen gaan verwijzen naar bibliotheken zodat ze daar digitaal goed en veilig hun zaken met de overheid kunnen regelen. Dit zaken doen gebeurt in de portalen van de Belastingdienst (MijnBelastingdienst.nl en MijnToeslagen) en de generieke overheidsvoorzieningen waar de Belastingdienst gebruik van maakt (MijnOverheid/Berichtenbox en DigiD). Daarom is in het convenant oa. de volgende bijdrage vanuit de Belastingdienst en KB opgenomen:

- De Belastingdienst stelt in overleg met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties de (veiligheids)eisen vast die aan de computers, het internetnetwerk en de printfaciliteiten bij de vestigingen van lokale bibliotheken worden gesteld, om goed digitaal zaken te kunnen doen via de portalen van de Belastingdienst en via MijnOverheid.
- De Belastingdienst biedt desgewenst ondersteuning aan de vestigingen van lokale bibliotheken bij het implementeren van de (veiligheids)eisen.
- De KB zal de lokale bibliotheken die een bijdrage als bedoeld in het tweede lid ontvangen, verplichten om de (veiligheids)eisen na te leven.

De bibliotheken zijn en blijven zelf verantwoordelijk voor de diensten, en de kwaliteit ervan, die ze aan burgers aanbieden om te internetten, deze verantwoordelijkheid neemt de Belastingdienst niet over.

Deze eisen worden geformaliseerd door de Belastingdienst en Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (vanwege de rol van de dienst Logius van dit ministerie als beheerder van MijnOverheid/Berichtenbox en DigiD) en de KB, door ze als voorwaarde op te nemen in de subsidieregeling voor bibliotheken.

Doel

Bibliotheken hebben ruime ervaring met informatiebeveiliging. Per vestiging kan hier een verschillende inrichting voor gelden, omdat de lokale situatie per bibliotheek verschilt (bijvoorbeeld een dorpsfiliaal versus een centrale stadsvestiging). Het convenant tussen de Koninklijke Bibliotheek en de Belastingdienst heeft (landelijk) gevolgen voor de informatiebeveiliging (zie hoofdstuk 2 over context). Deze notitie over (veiligheids)eisen, hierna (informatiebeveiligings)eisen[1] genoemd, heeft als doel om duidelijk te maken wat de Belastingdienst belangrijke aspecten vindt bij veilig digitaal zaken doen, onafhankelijk van de inrichting. Door dit expliciet te maken in (informatiebeveiligings)eisen hebben alle bibliotheken en de Belastingdienst een gemeenschappelijk referentiekader van wat de Belastingdienst verwacht van de voorzieningen in de bibliotheek. Vanuit dit referentiekader bepalen bibliotheken vervolgens, afhankelijk van de situatie op de vestiging, waar ze eventueel nog iets moeten aanpassen aan hun voorzieningen om te voorkomen dat misbruik of fraude in de hand wordt gewerkt. Uiteraard bepalen bibliotheken zelf *hoe* ze invulling geven aan de eisen. Aan de hand van deze eisen wordt ook gerapporteerd over de mate waarin veilig zaken doen met de Belastingdienst wordt ondersteund door de bibliotheek.

Deze eisen hebben geen betrekking op burgers die met eigen devices in de bibliotheek komen (bv. smartphone of tablet) en alleen gebruik maken van de wifi-verbinding van de bibliotheek om op internet te komen. De bibliotheek heeft wel een eigen rol om deze burgers waar nodig te attenderen of bewust te maken van privacy/informatiebeveiligingsaspecten bij internetten in de bibliotheek, maar dit staat los van het convenant tussen KB en de Belastingdienst. Dat heeft alleen betrekking heeft op burgers die naar de bibliotheek komen om vanaf een pc en internetverbinding van de bibliotheek hun zaken te regelen.

Verantwoordelijkheden

De opgestelde (informatiebeveiligings)eisen moeten worden gezien in het licht van de hierna genoemde verantwoordelijkheidsverdeling. In het implementatieplan, waarbij naast de Belastingdienst en KB, ook Provinciale OndersteuningsInstellingen (POI's) en uiteraard de lokale bibliotheken betrokken zijn, wordt een nadere invulling gegeven van de genoemde verantwoordelijkheden en worden waar nodig zaken nader vastgelegd. Denk onder andere aan de wijze van toetsing op voldoen en naleven van de (informatiebeveiligings)eisen, wie wanneer op welke wijze aan wie rapporteert, de manier waarop lokale bibliotheken worden ondersteund om aan hun verantwoordelijkheid invulling te geven. Ook wordt daarin vastgelegd hoe wordt omgegaan met issues en incidenten.

Burger

- De burger is verantwoordelijk voor de Belastingdienstzaken die hij in de bibliotheek uitvoert (bv. aangifte Inkomstenbelasting, wijziging Toeslagen).
- De burger is verantwoordelijk voor het zorgvuldig omgaan met zijn persoonlijke gegevens (inclusief wachtwoorden etc).
- De burger wordt geacht integer om te gaan met voorzieningen die in de bibliotheek aan hem ter beschikking worden gesteld en ze te gebruiken waarvoor ze bedoeld zijn.

De lokale bibliotheek (hierna bibliotheek genoemd)

- De bibliotheek is verantwoordelijk voor het bieden van gratis computer- internet en printfaciliteiten waarop de portalen/voorzieningen van de Belastingdienst/Logius functioneel werken.
- De bibliotheek is verantwoordelijk voor het inrichten van de organisatie, locatie, processen, communicatie en voorzieningen, conform de gestelde (informatiebeveiligings)eisen van de Belastingdienst.
- Bibliotheken rapporteren regelmatig of ze (nog) voldoen aan de (informatiebeveiligings)eisen. Dit gebeurt zowel tijdens de initiële implementatie (conform afspraken in het

[1] Deze term dekt de lading beter. Het gaat immers niet om veiligheid in brede zin, maar om het aspect informatiebeveiliging.

implementatieplan) als daarna (minimaal 1x per jaar). Daarbij wordt zoveel mogelijk gebruik gemaakt van of aangesloten op rapportageverplichtingen waaraan bibliotheken uit anderen hoofde moeten voldoen.

Koninklijke Bibliotheek

- De KB formaliseert de opgestelde (informatiebeveiligings)eisen door deze als voorwaarde op te nemen in de subsidieregeling voor de bibliotheken. Hij verplicht daarmee de bibliotheken om de (informatiebeveiligings)eisen blijvend na te leven.

- De KB draagt er blijvend zorg voor dat aan de Belastingdienst regelmatig wordt gerapporteerd in welke mate de bibliotheken voldoen aan de (informatiebeveiligings)eisen. Als er gevallen zijn van niet naleven van de (informatiebeveiligings)eisen, wordt aangegeven tot welke maatregelen dat heeft geleid.

Ministerie van Financiën, Belastingdienst

- De Belastingdienst maakt inzichtelijk wat nodig is voor functioneel goed werkende portalen (bv. http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/aangifte_doen/voorlopige_aanslag_nieuw/hoe_werkt_online_formulier_voorlopige_aanslag/browsers)
- De Belastingdienst stelt de (informatiebeveiligings)eisen op waaraan de bibliotheken moeten voldoen (zie onderdeel 2).
- Daar waar vragen zijn bij bibliotheken over de invulling van de eisen, ondersteunt de Belastingdienst (dit loopt via provinciaal of centraal niveau, zie implementatieplan).
- Daar waar in de toekomst de voorzieningen van de Belastingdienst zodanig wijzigen dat dat invloed heeft op de gestelde (informatiebeveiligings)eisen, gaat de Belastingdienst hierover met de KB in gesprek en worden de eisen waar nodig aangepast.
- De Belastingdienst zorgt ervoor dat eventuele wijzigingen in eisen tijdig bij de bibliotheken bekend zijn, zodat ze een reële termijn hebben om zich hierop voor te bereiden.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius

- Logius maakt inzichtelijk wat nodig is voor een functioneel goed en veilig werkend portaal MijnOverheid en goed werkende authenticatie- en autorisatievoorzieningen (op dit moment DigiD en DigiD Machtigen) voor burgers (bv www.digid.nl/veiligheid en https://mijn.overheid.nl/veiligheid).
- Logius staat waar nodig de Belastingdienst bij in het beantwoorden van vragen vanuit de bibliotheken over invulling van de gestelde eisen (bv via de helpdesk).
- Logius signaleert eventuele issues en nieuwe ontwikkelingen die betrekking hebben op (informatiebeveiligings)eisen en relevant zijn voor de Belastingdienst, KB/bibliotheken.

Hoewel de Belastingdienst dus niet verantwoordelijk is voor het naleven van de (informatiebeveiligings)eisen door de bibliotheken, heeft zij er groot belang bij dat een burger goed en veilig zaken kan doen bij de bibliotheek en dat de opgestelde (informatiebeveiligings)eisen zorgvuldig worden nageleefd. Eventuele incidenten waarbij achteraf blijkt dat (enkele) bibliotheken evident hun zaken niet op orde hadden, schaden niet alleen betrokken burgers en de betreffende lokale bibliotheken, maar kunnen ook landelijk grote impact hebben. Al zou de materiële schade van de incidenten beperkt zijn, ze kunnen ernstig het imago schaden van het landelijke samenwerkingsverband tussen KB, bibliotheken en Belastingdienst, evenals het vertrouwen van de burger om zijn digitale zaken in de bibliotheek te doen.

1. Context

Hierna wordt de context geschetst die relevant is voor de eisen die de Belastingdienst stelt naar aanleiding van het afgesloten convenant met de Koninklijke Bibliotheek.

Om welke gegevens gaat het bij digitaal zaken doen?
De focus ligt op het regelen van persoonlijke belastingen- en toeslagzaken met de Belastingdienst waarbij bijvoorbeeld de volgende gegevens ingezien kunnen worden of onderdeel zijn van transacties: inkomensgegevens, schulden, rekeningnummer, BSN, adres en telefoonnummer. Ook gaat het om inzage in correspondentie van de Belastingdienst en andere overheidspartijen en persoonlijke gegevens in MijnOverheid. Om toegang tot deze gegevens te krijgen moeten een burger zich authenticeren met DigiD (of zijn helper met DigiD Machtigen).

De voorzieningen van de Belastingdienst en Logius
Behalve dat Belastingdienst en Logius functioneel goed werkende portalen en voorzieningen beschikbaar stellen via internet, hebben zij ook een aantal informatiebeveiligingszaken ingebouwd om te voorkomen dat persoonlijke gegevens gemakkelijk in handen van derden kunnen vallen (bv. beveiligde internetverbinding, automatisch beëindigen inlogsessie na bepaalde tijd van inactiviteit).

Huidige situatie bij de bibliotheken
Veel bibliotheken voorzien al een hele tijd in internetplekken (en ook vaak printers) voor burgers, soms tegen betaling. Burgers gebruiken deze nu bijvoorbeeld om een digitale krant te lezen, informatie te zoeken, te gamen, te e-mailen, online te bankieren of shoppen. Ze kunnen nu ook al digitaal zaken doen met de Belastingdienst en andere overheidsorganisaties. Bibliotheken hebben ruime ervaring met het beveiligen van internetvoorzieningen en het voorkomen van misbruik. De invulling verschilt per bibliotheek en hangt ook samen met het type internetgebruik. Het verschil met de situatie onder het convenant is dan ook niet zozeer gelegen in de geboden voorzieningen en de veiligheid daarvan, maar in het feit dat het gebruik voor zaken doen met de overheid in alle gevallen gratis is.

Wat verandert er?
Of een burger een bibliotheek opzoekt om zijn digitale zaken te doen is de keuze en de verantwoordelijkheid van de burger. Vanwege de afspraak tussen de Belastingdienst en de KB om burgers te wijzen op de mogelijkheid om in de bibliotheek gratis digitaal hun zaken te doen, en er naar verwachting structureel meer gebruik zal worden gemaakt van de bibliotheekvoorzieningen, moet de burger er op kunnen vertrouwen dat de informatiebeveiliging bij de bibliotheken in het land goed is geregeld.
In het onderstaande wordt een aantal aspecten gegeven die voor dit vertrouwen van belang zijn. In de volgende paragraaf wordt dit uitgewerkt in concrete eisen.

- De burgers die gebruik gaan maken van de computers en internetfaciliteiten in de bibliotheek, zullen een beneden gemiddelde kennis van ICT hebben. In de bibliotheek hebben ze geen inzicht in ICT-inrichting en ook geen invloed hierop. Zij moeten erop kunnen vertrouwen dat dit goed is geregeld.

- De bibliotheek kent verschillende typen internetgebruik van burgers, waardoor een maatregel die geschikt is voor het ene type gebruik juist ongeschikt is voor een ander type gebruik. Een voorbeeld is het bevorderen (of niet verhinderen) van het kunnen meekijken op een internetplek, om te voorkomen dat burgers ongewenste sites raadplegen of ongewenste handelingen uitvoeren. Voor het digitaal zaken doen met de Belastingdienst/overheid is het juist belangrijk dat de burger privacy heeft.

- Een burger in de bibliotheek bevindt zich in een openbare ruimte. Hij zal zich niet altijd realiseren dat zijn persoonlijke gegevens gemakkelijker in handen van anderen kunnen vallen

(per ongeluk of met opzet) dan thuis in de privésfeer. Ook zal hij zich niet altijd realiseren dat hij daar zelf een grote rol in speelt.

- Een burger die door de Belastingdienst wordt verwezen naar de bibliotheek kan de indruk krijgen dat de bibliotheek een soort verlengstuk van de Belastingdienst is en denken dat bibliotheekmedewerkers dezelfde competenties en bevoegdheden hebben als Belastingdienstmedewerkers en gemachtigd zouden zijn om iets met zijn gegevens te doen. Dit zou ertoe kunnen leiden dat hij spontaan aangifte-issues gaat voorleggen aan een bibliotheekmedewerker. Dat kan zowel de burger als de bibliotheekmedewerker in een vervelende positie brengen.

- Als iemand thuis een print maakt, heeft hij daar zelf regie over en bevindt hij zich in een private ruimte. Als iemand in bibliotheek een print maakt, afhankelijk van inrichting en verloop van het printproces (inclusief eventuele verstoringen), is de privacy van de burger voor zijn prints minder geborgd.

- In de samenwerkingsrelatie waar het convenant over gaat, zijn behalve bibliotheken en burgers ook maatschappelijk dienstverleners betrokken. Maatschappelijk dienstverleners helpen burgers met het daadwerkelijk zaken doen met de Belastingdienst, bijvoorbeeld het invullen van een belastingaangifte of wijzigen van gegevens voor toeslagen. Een burger kan een maatschappelijk dienstverlener meenemen naar de bibliotheek en gebruik maken van de computer-, internet- en printvoorzieningen van de bibliotheek of een burger en maatschappelijk dienstverlener kunnen deelnemen aan belasting- en toeslagspreekuren die de bibliotheek faciliteert. Relevant is dat de hulpverleningsrelatie tussen burger en maatschappelijk dienstverlener niet anders is binnen de bibliotheek dan daarbuiten. Burger en helper regelen zelf hun hulpverleningsrelatie en hoe ze die invulling geven (bijvoorbeeld door de maatschappelijk dienstverlener te (laten) machtigen of door hem te laten meekijken), daar heeft de bibliotheekmedewerker geen verantwoordelijkheid of rol in. De burger blijft verantwoordelijk voor wat hij doet, al dan niet ondersteund door een maatschappelijk dienstverlener. In het geval de maatschappelijk dienstverlener geen gebruik gemaakt van voorzieningen van de bibliotheek maar zijn eigen voorzieningen meeneemt, geldt hiervoor hetzelfde als voor burgers die dit doen (zie kopje ‘doel’).

2. (Informatiebeveiligings)eisen

De (informatiebeveiligings)eisen[2] betreffen de eisen voor functioneel goed en veilig werkende voorzieningen en het waarborgen van de privacy van de burger die de bibliotheek bezoekt om gebruik te maken van de pc's, internet en printvoorziening. Ze dienen nageleefd te worden bij:

- Goedpad: bij normaal functioneren van voorzieningen;
- Foutpad: bij foutsituaties (bv. computer / printer loopt vast).

Functioneel

1) De computer is uitgerust met een operating system en een gangbare browser waarmee een beveiligde internetconnectie kan worden aangegaan om zaken te doen in de portalen van de Belastingdienst met gebruik making van de voorzieningen van MijnOverheid (met name DigiD en Berichtenbox) en er wordt toegang geboden tot printfunctionaliteit (internetplek).

Basis ICT

2) Het operating system en de browser zijn up-to-date, uitgerust met de laatste versie van de leveranciers.

3) De internetplekken zijn uitgerust met een virusscanner en firewall die up-to-date zijn.

4) De internetplekken zijn zodanig ingericht dat er geen eigen executables op neergezet/uitgevoerd kunnen worden door de burger (voorkomen installeren van malware, mobile browsers etc.).

5) De internetplekken zijn zodanig ingericht dat er geen (sporen van) persoonlijke gegevens/bestanden van een burger kunnen achterblijven nadat hij zijn sessie heeft beëindigd (inclusief sessie- en browsergegevens).

6) De fysieke hardware is zo veilig mogelijk, o.a. geen draadloze muizen/toetsenborden.

Positionering internetplekken op de locatie

7) De internetplekken en printers zijn zodanig gepositioneerd in de ruimte dat gemakkelijk meekijken op het scherm met de burger door een andere burger of bibliotheekmedewerker zoveel wordt voorkomen. Bv. geen gemakkelijke meekijk vanuit de looproute, (tussen)schotjes als pc's dicht bij elkaar staan of dichtbij andere plekken waar mensen zijn/zitten.

8) De internetplekken zijn zodanig ingericht dat wordt voorkomen dat prints in te zien zijn/in handen komen van andere burgers. Er wordt zoveel mogelijk voorkomen dat bibliotheekmedewerkers hier inzage/toegang toe krijgen. Als dat laatste wel nodig is: zie volgend punt.

Bibliotheekmedewerker

9) Mocht het vanwege de inrichting van het proces, hetzij in de goedsituatie hetzij in foutsituaties (bv. vastlopen van een pc of printer) noodzakelijk zijn dat een bibliotheekmedewerker een rol speelt in het (herstel)proces en daardoor inzage heeft in persoonlijke gegevens van de burger, wordt verzekerd dat deze medewerker de persoonlijke gegevens van de burger waar hij eventueel toegang tot krijgt, niet gebruikt/deelt met anderen (bv. verklaring geheimhoudingsplicht).

[2] Zie eventueel voor best practices bij deze richtlijnen ISO-norm 27001 over informatiebeveiliging.

10) De bibliotheek(medewerker) informeert de burger voor deze begint met zijn internetsessie over veilig digitaal zaken doen met de Belastingdienst. Dit kan bijvoorbeeld door het communiceren (en laten accepteren) van gebruiksvoorwaarden, het geven van (digitale) instructies of informatie. Het gaat hierbij over:

- wijzen op eigen verantwoordelijkheid voor het zorgvuldig omgaan met zijn persoonlijke gegevens, alert zijn op eventueel meekijkgedrag van anderen in de bibliotheek, expliciet uitloggen voor vertrek, zelf erop toezien dat hij resultaten van printopdrachten in ontvangst neemt en eventuele overbodige printopdrachten annuleert of laat annuleren voordat hij weggaat.
- attenderen op het feit dat de portalen van de Belastingdienst tussentijdse opslag ondersteunen, zodat het niet erg is als de burger niet in één sessie zijn zaken kan doen en ook niet afhankelijk (juist niet!) is van een opslagmogelijkheid op de internetplekken;
- verwijzen naar waar de burger terecht kan als hij merkt moeite te hebben met bepaalde deelgebieden, bv. DigiD aanvragen of activeren Berichtenbox, belasting- of toeslagzaken. Dit kunnen zijn de dienstverleningskanalen van de Belastingdienst en MijnOverheid, maatschappelijk dienstverleners met wie de bibliotheek hierover afspraken heeft gemaakt, of het cursusaanbod digitale vaardigheden bij de bibliotheek;
- de rol van de bibliotheekmedewerker, die alleen bestaat uit het wegwijs maken met computer/printer, en niet uit het beantwoorden van vragen over Belastingen en Toeslagen of het gebruik van de portalen MijnBelastingdienst, MijnToeslagen, MijnOverheid en zijn DigiD.
- signaleren bij een bibliotheekmedewerker als de burger iets afwijkends of vreemds ziet of persoonlijke gegevens (bv. printje dat is achtergebleven) van een andere burger tegenkomt.

11) Daar waar een bibliotheekmedewerker, al dan niet door het signaal van een burger, persoonlijke gegevens van een burger aantreft op een verlaten internetplek of printer (bv een printje of briefje met wachtwoorden), draagt hij zorg voor zorgvuldige vernietiging hiervan om te voorkomen dat andere burgers of medewerkers deze gegevens kunnen inzien. Afhankelijk van de situatie, bv in geval van een achtergebleven brief van een overheidsinstantie of bank, kan een bibliotheekmedewerker ervoor kiezen de gegevens (tijdelijk) op een veilige plek te bewaren voor het geval de burger zelf nog terug zou komen of kan hij eventueel contact leggen met de burger. Als de gegevens niet binnen een redelijke termijn aan de burger kunnen worden teruggegeven, worden ze alsnog vernietigd.

12) Daar waar een bibliotheekmedewerker een inbreuk op de beveiliging of een datalek op de internetwerkplek vermoedt, meldt hij dat bij het daarvoor aangewezen aanspreekpunt binnen de bibliotheek. De bibliotheek moet vervolgens zelf besluiten of er sprake is van een datalek in de zin van Wet bescherming persoonsgegevens dat hij binnen 72 uur moet melden aan de Autoriteit Persoonsgegevens. De afweging om waar het incident de Belastingdienst raakt, dit bij de Belastingdienst te melden, maakt onderdeel uit van de eigen standaardprocedure die daarop volgt. Bij incidenten in de bibliotheek die de Belastingdienst raken, wil de Belastingdienst zo vroeg mogelijk betrokken zijn, om eventueel te handelen en ook om te voorkomen dat deze pas laat door derden (bijvoorbeeld de pers) bij ons bekend worden.