B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Algemene bepalingen AWR?

1. Verwerking van de persoonsgegevens door de Belastingdienst ten behoeve van zijn wettelijke taken in de fiscaliteit en toeslagen: artikel 6 lid 1 onder e AVG.
2. Artikel 6 lid 1 onder f AVG; gerechtvaardigd belang; hoewel er beperkt voorbeelden[12] zijn gebleken van inzet van FSV trendanalyses en BI ten behoeve van de bedrijfsvoering, is dit wel een beoogde inzetvorm.
3. Registratie van verstrekking op verzoek van persoonsgegevens door de Belastingdienst aan derden met een wettelijke taak: artikel 6 lid 1 onder c AVG. (de informatieverzoeken). Het volledige proces van de externe informatieverzoeken is behandeld in de GEB Informatieloketten. Hier wordt alleen het aspect registratie (en eventuele verdere verwerking) in FSV bedoeld.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

[12] Toeslagen gebruikt FSV ook om te raadplegen bij Bibob en Track verzoeken. Omdat Toeslagen in FSV het Gefisnr. (th. PSF) registreert en het boetebedrag en percentage in FSV registreert. Dit valt onder het kopje strafrechtelijke gegevens.

1. **Informatieverzoeken** bevatten mogelijk **bijzondere**[13] persoonsgegevens. De primaire verwerking (het afhandelen van het informatieverzoek) voldoet aan de voorwaarden voor verwerking van art. 9 onder f en g AVG. De verdere verwerking van aangaande het informatieverzoek binnen FSV en evt. andere informatiesystemen moet aanvullend en indien van toepassing herhaald getoetst worden. De context in combinatie met (de betekenis van) de gegevens is bepalend voor de wijze van gebruik. Een informatieverzoek is bv. niet op voorhand / op per definitie een (fraude)signaal en de actualiteitswaarde begrenst. De huidige verwerkingswijze is hierop onvoldoende ingericht.
2. **Tips en kliks**[14] (signalen) ontvangen van derden kunnen **bijzondere** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt deze signalen bij de uitvoering van zijn taken 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. De primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze is hierop onvoldoende ingericht.
3. **Interne en externe**[15] **(fraude) signalen** kunnen **bijzondere** persoonsgegevens bevatten. De primaire verwerking (het afhandelen van de tip/klik) voldoet aan de voorwaarden voor verwerking van art. 9 onder g AVG. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor alle gevallen zondermeer aanwezig. De huidige verwerkingswijze is hierop onvoldoende ingericht. Toeslagen boekt onder "aangifte fraude" de signalen in, op het moment dat er een gerede twijfel is aan de opmaak van documenten (facturen, contracten, etc.) hier is al een kort onderzoek aan vooraf gegaan. Dit kan door een andere afdeling zijn gedaan of afkomstig zijn van externe partijen (zie 4.) of een klikmelding (zie 2.).
4. **Informatieverzoeken** bevatten **strafrechtelijke** persoonsgegevens. De wettelijke uitzondering voor verwerking is primair gelegen in de wettelijke grondslag (lees verplichting) bijvoorbeeld een vordering op grond van art. 126nd Sv. Daarmee voldoet de verwerking 'in enge zin' (ten behoeve van het voldoen aan de vordering) aan de voorwaarden[16] voor verwerking van art. 10 AVG jo art. 23 onder c UAVG. De verdere verwerking binnen FSV en evt. andere informatiesystemen voldoet aan de voorwaarde van 'verwerking onder toezicht van de overheid'. De context van een informatieverzoek in combinatie met (de betekenis van) de gegevens is wel bepalend voor de wijze van gebruik. Een extern informatieverzoek is niet bedoeld te gelden als / niet op voorhand / per definitie een (fraude)signaal en de actualiteitswaarde is begrenst. Toeslagen doet bij gerede twijfel eerst onderzoek en voert dan evt. een signaal op. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd. De aanpak van Toeslagen kan, indien dit past binnen het uitvoeringsproces, hierbij als uitgangpunt worden genomen.
5. **Tips en kliks** ontvangen van derden kunnen **strafrechtelijke** persoonsgegevens bevatten. De Belastingdienst ontvangt en verwerkt dit 'spontaan' doordat derden signalen moeten kunnen aanbrengen over andere burgers. Ook hier is bij aanvang van de verwerking sprake van de uitzondering 'onder toezicht van de overheid'. De verdere verwerking is wel aan beperkingen onderhevig incl. dit plicht tot vernietiging bijvoorbeeld bij gebleken onbruikbaarheid of onjuistheid. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.
6. **Interne (fraude) signalen** kunnen **strafrechtelijke** persoonsgegevens bevatten (waaronder daarmee gelijkgeschakelde fiscale sanctiegegevens). Ook hier geldt dat bij aanvang van de verwerking strafrechtelijke gegevens sprake is van de uitzondering 'onder toezicht van de overheid'. In de verdere verwerking speelt de context en kwaliteit van de gegevens een bepalende rol voor de rechtmatigheid en welbepaaldheid van de verdere verwerking. Die is niet voor

alle gevallen zondermeer aanwezig. De huidige verwerkingswijze moet ten aanzien van deze aspecten worden verbeterd.

7. Bovenstaande geldt ook voor projecten gebaseerd op gegeven zoals besproken onder 1 tot en met 6.
8. Gegevens met een **'zwarte lijst'**-karakter: in FSV ontstaan of worden bestaande gegevenselementen verwerkt die het karakter van een zwarte-lijst-element hebben of krijgen. De mogelijke subjectiviteit ('bias', vooringenomenheid, zelfversterkend effect door stapeling) maakt het verwerken risicovol. Ook het voorkomen in FSV als betrokkene wordt als risicosignaal. Dit brengt ook een aantal risico's met zich mee waaronder een mogelijk 'zwarte lijst'-effect.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

---

[13] Direct of indirect. Bv. in de context van zorgtoeslag kan een gegeven indirect iets over de gezondheidstoestand van een betrokkene zeggen.

[14] Tips/kliks is een algemeen begrip. In het signaal moet worden opgenomen wat de bron. Via overzichten kunnen aantallen (per periode, kantoor, BSN/RSIN) inzichtelijk worden gemaakt.

[15] Zoals MMA, Track/Justis, FIU, iSZW e.d.

[16] "..verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unitrechtelijke of lidstaatrechtelijke bepalingen die voldoende waarborgen ... bieden." Zorgtoeslag van Toeslagen is een tegemoetkoming in de kosten voor een zorgverzekering, die inkomensafhankelijk is.

De vraag of de verdere gegevensverwerking verenigbaar is met het oorspronkelijke verzameldoel van de gegevens, speelt met name met betrekking tot de verdere verwerking gegevens in FSV. De initiële vastlegging van persoonsgegevens bij (registratie van) een informatieverzoek of (extern) tip/klik/signaal of intern signaal is namelijk het begin van de verwerking. Vanwege het verschillende karakter worden informatieverzoeken apart behandeld naast de (fraude)signalen.

Informatieverzoeken: In deze afweging zijn de volgende factoren gewogen:

a. Het verband tussen het oorspronkelijk verzameldoel en de doeleinden van de voorgenomen verdere verwerking;
b. Het kader waarin de persoonsgegevens zijn verzameld en de redelijke verwachtingen van de ontvanger (de betrokkene) met betrekking tot de voorgenomen verwerking;
c. De aard van de persoonsgegevens en met name of bijzondere persoonsgegevens worden verwerkt;
d. De mogelijke gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene);
e. Het bestaan van passende waarborgen, waaronder versleuteling of pseudonimisering van de gegevens.

Ad a. Het informatieverzoek wordt verwerkt (geregistreerd) wanneer een externe overheidspartij op basis van een wettelijke grondslag inlichtingen vordert. Het verwerkingsdoel is tweeledig:

1. Vastlegging van (een deel van de[17]) informatie aangaande het informatieverzoek ten behoeve van een goede verwerking van het verzoek en het creëren van een audit trail.
2. Vastleggen van contra-informatie/renseignementen vanuit het (ten dele statistisch onderbouwde) ervaringsgegeven[18] dat een significant deel van subjecten waarvan informatie wordt opgevraagd, fiscaal gezien aanvullende aandacht verdient of mogelijkheid dat de betrokkene ook fiscaal nader onderzocht of getoetst moet worden. (Vermoedens van) misbruik doet zich veelal regeling overstijgend voor én er is een wederzijdse relatie doordat inkomen- en vermogen (mede)bepalend is voor aanspraken op diverse regelingen buiten de fiscale context.

De verdere verwerking zal plaatsvinden doordat bij de risico(posten)selectie en/of individuele klantbehandeling FSV direct of indirect (via export van FSV-data naar andere bronnen) wordt geraadpleegd. Het gebruiken van FSV als bron is verenigbaar indien kan worden gegarandeerd dat de gegevensset juist, volledig en actueel is en de gegevens inclusief contextinformatie worden verwerkt. Een informatieverzoek heeft bv. een andere context en daardoor betekenis dan een kliksignaal.

Er is vastgesteld dat deze zorgvuldigheid bij de huidige inrichting niet voldoende kan worden gegarandeerd. Zo wordt per bedrijfsonderdeel en daarbinnen per behandelend team (en mogelijk individu) anders omgegaan met de mate van vastlegging in FSV. Ook de verdere verwerking van FSV data in andere informatiesystemen is voldoende fijnmazig. Als het überhaupt voorkomen in FSV als selectiecriterium geldt, wordt geen rekening gehouden met de context en hiervan afgeleid met mogelijk (onterechte) stigmatisering van betrokkenen als gevolg.

Ad b. Het vastleggen van een informatieverzoek vloeit voort uit een wettelijke plicht. De betrokkene zal in het merendeel van de gevallen hiervan niet (direct) op de hoogte zijn maar via het dossier (strafdossier, alimentatie-dossier LBIO) op enig moment geconfronteerd worden met het feit dat een dergelijke verwerking heeft plaatsgevonden. De Belastingdienst informeert de ontvanger (betrokkene) in zijn algemeenheid door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

Ad c. Er worden bijzondere- en strafrechtelijke persoonsgegevens verwerkt evenals een wettelijk identificatienummer (BSN). De aard en het karakter van dit type verwerking brengt dat met zich mee. Dit brengt extra zorgvuldigheidseisen met zich mee uitgaande van wettelijke

mogelijkheden (zo niet verplichting) om deze gegevens te verwerken.
Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een informatieverzoek in FSV, zonder fiscale relevantie vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.
Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst zonder pseudo- of anonimisering. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolafhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

(Fraude/klik/tip)Signalen: De signalen vormen de tweede groep die beschouwd zal worden in deze paragraaf. Hoewel verschillend qua typologie vormen ze wel één groep die zich onderscheidt van de informatieverzoeken.
Ad a. De geregistreerde signalen van fraude/misbruik worden gebruikt voor (ruwweg) risicoselectie en de klantbehandeling. Bij signalen van derden ligt het initiatief bij (anonieme) burgers en komen van andere (overheids)Partners af, interne signalen komen op vanuit de verschillende bedrijfsprocessen rondom de klantbehandeling (fiscaal en toeslagen). Verwerking vindt steeds plaats in de context van het bevorderen van compliantie van betrokkenen.
Ad b. Hoewel de Belastingdienst de betrokkene in zijn algemeenheid informeert door middel van het privacy statement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst", is de specifieke verwerking van signalen in FSV voor het merendeel van de betrokken onbekend. Indirect wordt een betrokkene hier op enig moment mee bekend doordat er een vorm van (geïntensiveerde) klantbehandeling ontstaat waarin FSV mede bepalend is geweest.
Ad c. Er worden mogelijk en in voorkomend geval bijzondere en strafrechtelijke persoonsgegevens verwerkt evenals het BSN als wettelijk identificatienummer.
Ad d. De gevolgen van de voorgenomen verwerking voor de ontvanger (betrokkene) kunnen groot zijn. Als de enkele registratie van een signaal in FSV leidt vervolgens meerjarig (tot nu toe zelfs blijvend vanwege het ontbreken van een verwijdermogelijkheid) geldt als variabele in diverse risicoprofielen van de Belastingdienst, dan herbergt dit het risico van te grofmazige risicoselectie en mogelijke stigmatisering.
Ad e. De gegevens worden verwerkt binnen de beveiligde infrastructuur van de Belastingdienst. Het relatief grote aantal personen dat toegang heeft tot de gegevens (raadplegen en evt. muteren, rolafhankelijk) zonder een goed ingerichte need-to-know-structuur en het ontbreken van logging en monitoring vormt daarbinnen een risico.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. **Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?**
b. **Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.**

---

[17] In veel gevallen wordt in FSV alleen een signaal vastgelegd en worden onderliggende stukken elders opgeslagen. Dit wordt voornamelijk ingegeven door het grote aantal autorisaties op FSV en het daardoor ontstane overschrijden van een need-to-know-toegang tot signaalinformatie.
[18] Bron: DF&A

a. Proportionaliteit:
Vanwege het verschillende karakter worden ook hier informatieverzoeken onderscheiden behandeld van de (fraude)signalen.

Informatieverzoeken: de inbreuk op de privacy wordt gerechtvaardigd doordat de afhandeling van een informatieverzoek voortvloeit uit een wettelijke plicht. Vanuit een zorgvuldigheidsoogpunt is registratie een noodzakelijke processtap. De noodzakelijkheid van de (verdere) verwerking buiten de 'logistieke' doeleinden van het zorgvuldig afhandelen van een informatieverzoek vraagt om aanvullende, privacy-bevorderende maatregelen. De noodzaak van verdere verwerking van een informatieverzoek als renseignement moet zorgvuldig worden getoetst én vraagt om vastlegging van voldoende (en hierdoor mogelijk verwerking van meer) (persoons)gegevens om bij de verdere verwerking de relevantie te kunnen bepalen. Tevens moet de 'houdbaarheid' voldoende fijnmazig worden bepaald. Ieder (type) informatieverzoek heeft zijn eigen, beperkte, actualiteitswaarde. Er moet een goed evenwicht gevonden worden tussen ervaringsregels als 'een signaal is geen signaal' en 'waar rook is, is vuur' die ieder voor zich leiden tot het verlengen van de bewaartermijnen en de belangen en rechten van betrokkenen. De werkwijze van Toeslagen, waarbij een informatieverzoek wordt 'gewogen' en bij gerede twijfel FSV wordt 'aangevuld' met een signaal lijkt een zuivere scheiding tussen een informatieverzoek en een signaal te kunnen aanbrengen.

(Fraude/klik/tip)Signalen: de inbreuk op de privacy wordt in zijn algemeenheid gerechtvaardigd doordat het ontvangen of intern ontstaan van signalen een logisch gevolg is van de uitvoering van de wettelijke taken van de Belastingdienst. Signalen van derden (tips/kliks en andere signalen) zijn vormvrij, wat maakt dat een uniforme vastlegging georganiseerd moet worden. FSV is hiervoor een instrument. De criteria voor registratie in FSV laten toe dat de mate van 'hardheid', objectiviteit / subjectiviteit, bruikbaarheid en actualiteit per melding verschilt zonder dat dit in de verdere verwerking als objectieve criteria toetsbaar is. Dit vraagt om aanvullende, privacy-bevorderende maatregelen die een betere balans geven in de plicht om een zo beperkt mogelijke privacy-schending te veroorzaken en tegelijkertijd de noodzaak tot het registreren van (mogelijk) fiscaal relevante signalen blijvend mogelijk te maken.

b. Subsidiariteit:
De verwerkingsdoelen voor beide informatiestromen kunnen met een aangepaste verwerkingswijze in FSV leiden tot hetzelfde resultaat maar met een minder grote inbreuk op de persoonlijke levenssfeer van betrokkenen. De mate waarin dit in de huidige opzet van FSV mogelijk en wenselijk is of bv. in de vorm van een migratie naar een nieuwe omgeving/voorziening, zal nader beoordeeld moeten worden.

De belangrijkste aspecten, grotendeels corresponderend met de hierna in paragraaf 16 te benoemen risico's, zijn: het aanbrengen van een beter onderscheid tussen informatieverzoeken en 'echte' signalen. de bewaartermijn, registratie en meeleveren van metadata (contextinformatie) ten behoeve van de verdere verwerking en need-to-know/have toegang van medewerkers.

15. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Het karakter van de verwerkingsgrondslagen voor opname van (persoons)gegegevens in FSV zal er in veel gevallen toe leiden dat bij een eventueel inzageverzoek betrokkene geen specifieke informatie, zoals verwerkt in en vanuit FSV, zal ontvangen. Een wettelijke geheimhoudingsplicht (bijvoorbeeld voortvloeiend uit art. 126nd SV maar ook specifieke signalen zoals MeldMisdaadAnoniem) kan hieraan in de weg staan maar ook de voorlopige geheimhouding corresponderend met de wettelijke taken van de (rijks)Belastingdienst. Art. 23 AVG, in het bijzonder letter d en h AVG geldt hier als beperking op de rechten van betrokkene.

Wel informeert de Belastingdienst de ontvanger (betrokkene) in zijn algemeenheid met betrekking tot in FSV registreerde persoonsgegevens door middel van het privacystatement en de brochure "Overzicht verwerkingen van persoonsgegevens door de Belastingdienst".

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

1. In zijn algemeenheid kan worden geconcludeerd dat **de huidige opzet van FSV geen goede aansluiting (meer) heeft op de verwerkingsbeginselen van art. 5 AVG.** Ten aanzien van elk van de 10 in dit artikel genoemde beginselen zijn een of meer bevindingen gedaan en afgeleid daarvan zijn er privacy risico's gesignaleerd. Hieronder worden de meest impact hebbende risico's beschreven. De hoofdmaatregel genoemd in .17 sluit overigens specifiek aan op dit eerste 'meta-risico'.

2. **Onvoldoende onderscheid tussen een informatieverzoek en een signaal maar ook betekenis/gewicht van de informatie, leidt tot mogelijke stigmatisering van betrokkene ('zwarte lijst effect').** FSV biedt de mogelijkheid tot registratie van beide fenomenen wat bij de (verdere) verwerking, afhankelijk van de wijze van verwerking, door de individuele gebruiker (of bedrijfsonderdelen) tot een verschillende en deels risicovolle verwerking leidt. Een afgeleid risico ontstaat doordat er nauwelijks of geen onderscheid wordt gemaakt in de kwalificatie, 'gewicht' en betekenis van een melding. Een informatieverzoek zonder fiscale relevantie 'weegt' even zwaar als een 'vage' klikmelding ('buurman

drie keer met een aanhangwagen met 'handel' zien rijden') of een concrete melding van bv. een valse factuur. Zeker wanneer de FSV content integraal (verder) wordt verwerkt en/óf de registratie in FSV als risicofactor wordt (mee)gewogen, is de kans groot dat een deel van de betrokkenen onterecht of bovengemiddeld snel/vaak als risicopost wordt aangemerkt met als gevolg een mogelijk meer intensieve klantbehandelingsvorm dan noodzakelijk is.

3. **De datakwaliteit vormt een risico** doordat registratie in FSV niet uniform geschiedt, het onderscheid tussen objectieve en subjectieve informatie onvoldoende inzichtelijk is en verouderde informatie blijvend wordt verwerkt. De oorzaak van voornoemde voorbeelden is verschillend. Respectievelijk de verschillende werkwijze van bedrijfsonderdelen (én teams en per medewerker), feiten en vermoedens (waaronder het label 'besmet adres') die deels zonder nadere kwalificatie/onderscheid worden verwerkt en het ontbreken van massale-archiverings-/schoningsfunctionaliteit. Dit heeft tot gevolg dat er een incompleet, onjuist en/of gedateerd beeld van betrokkene ontstaat in de (verdere) verwerking van gegevens, ook buiten FSV, zoals de risicopostenselectie (bv. bij DF&A) en toetsing in FSV in geval van individuele klantbehandeling. Dit kan aanzienlijke gevolgen hebben voor betrokkenen.

4. **Informatiebeveiligingsissues waaronder onvoldoende garantie ten aanzien van data-integriteit, vormen een risico** door te ruime toegang tot en onvoldoende controle op het gebruik van de gegevens in FSV. Er zijn inmiddels 5000+ medewerkers geautoriseerd[19] voor minimaal raadpleegtoegang tot alle data. Enkele rollen kunnen een export van de volledige database maken zonder zicht op de verdere verwerking van de geëxporteerde data. Er bestaat de mogelijkheid voor medewerkers met muteerrechten tot wijzigen (aanvullen, wijzigen, ante-dateren etc) van alle data in FSV. Dit wordt niet gelogd en gemonitord. Ook leidt voornoemde in zekere zin tot een zgn 'chilling effect'[20] doordat meerdere teams FSV slechts beperkt vullen ('hit-no hit-achtig') en een parallelle administratie voeren voor de details van het signaal. Hoewel er geen voorbeelden van incidenten/misbruik bekend zijn, voldoet de huidige verwerkingsvorm niet aan de eisen die, mede vanuit privacy by design/default, aan informatiesystemen worden gesteld. Ook hier bestaat een aanzienlijke kans dat de inbreuk op de privacy groter is dan noodzakelijk en de impact aanzienlijk kan zijn als er (veelal een verdere) verwerking ontstaat door de wijze van registratie in FSV.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

---

19 Waarvan ongeveer 10% (509) inactief, dd dec 2018.

20 Fenomeen dat ontstaat als personen zich anders gaan gedragen vanwege een mogelijke privacy-impact. Doorgaans betrokkene (belastingplichtigen), in dit geval medewerkers.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Als hoofdmaatregel wordt een herontwerp / migratie van FSV naar een nieuwe opzet[21] geadviseerd. Daarmee kunnen, met als uitgangspunt privacy by design en default, de gesignaleerde risico's worden weggenomen. Borg dat de migratie wordt gedaan in combinatie met processuele maatregelen als procesuniformering[22], work-flow-management, zicht en zeggenschap op en over de verdere verwerking van data buiten FSV en voldoende controle daarop.

Herontwerpaspecten gerelateerd aan privacy-risico's zijn dan: gegevenskwaliteit (metadatering van de betekenis / waarde van gegevens waaronder het 'gewicht' van een signaal en het onderscheid tussen een signaal en een informatieverzoek), ontwikkelen van systeemfunctionaliteit en vastleggen van meta-data met betrekking tot de bewaar/archiveringstermijn, organiseren en reguleren van (al dan niet geautomatiseerde[23]) datadistributie, need-to-know toegang tot data, logging- en monitoring van gebruik.

Mede afhankelijk van het tijdpad van de voorgestelde migratie/herontwerp, moet een aantal voorlopige maatregelen in de huidige opzet van FSV worden genomen, in het bijzonder ten aanzien van:

1. Het toetsen van de bestaande autorisaties (en mogelijk het aantal rollen) op noodzakelijkheid en actualiteit/geldigheid gevolgd door 'schoning' op basis van de uitkomst van de toetsing.
2. Het schonen van een aantal jaarlagen (bv jongste signaal over betrokkene is > x jaar).
3. a. Het aanbrengen van onderscheid tussen een signaal en een informatieverzoek bij verdere verwerking van FSV data in andere informatiesystemen / analyseomgevingen.
   b. (indien mogelijk) het zo objectief mogelijk vastleggen van het 'gewicht' van een signaal.
   c. Implementeren van een uniforme werkwijze (bv. Conform/analoog proces Toeslagen) om op fiscale relevantie onderzochte informatieverzoeken op te voeren als signaal en deze signalen (verder) te verwerken in plaats van de informatieverzoeken.
4. Het verwijderen/de-activeren (of nader beperken qua gebruikersgroep)van massale en/of integrale exportfunctie(s).
5. Verbeteren van kennis en gebruik van FSV in het bijzonder ten aanzien van de mogelijke privacyrisico's zoals stigmatisering. Hier kan ook worden gedacht aan een Code of Practice/gebruikersinstructie met ethische en privacy uitgangspunten, mogelijk in een breder verband dan FSV.

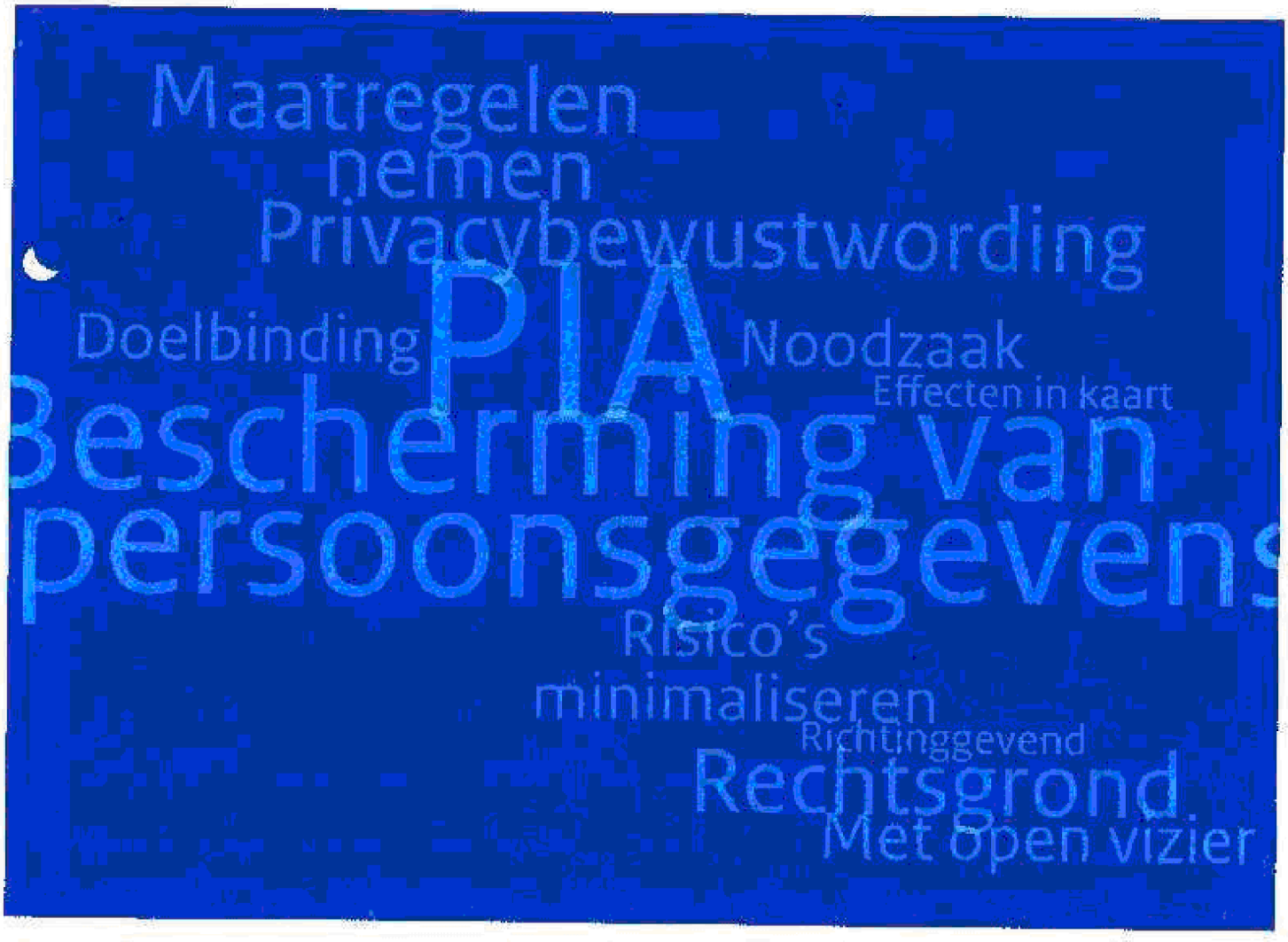
Maak hierbij gebruik van de al aanwezige informatie in het document 180329 F18.045 Feature aanpassingen Dagboek FSV en eerder vastgelegde oplossingsmogelijkheden voor herbouw.

---

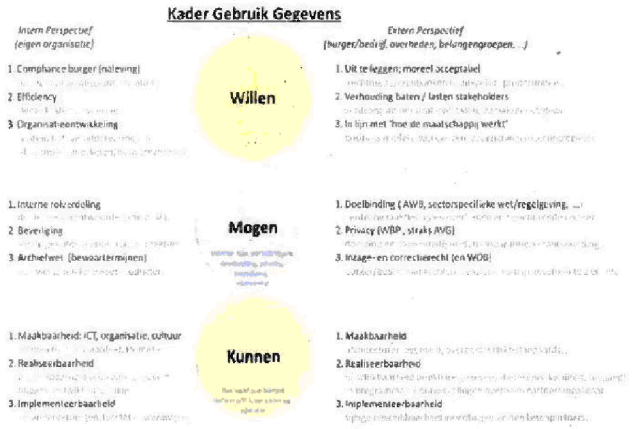
21 Mede ingegeven door de constatering dat er functionele wensen bestaan, soms overlappend met de in de PIA geadresseerde issues, die niet (goed) in de huidige applicatie-architectuur kunnen worden uitgewerkt. Kostenefficiëntie speelt mede een rol bij dit advies. Hierbij is aansluiten bij het project (in opstartfase) vanuit het Breed Informatiestroomlijn Overleg (BIO) gewenst. Het BIO heeft directe aansluiting op het concernbrede fraudelandschap (FDO, FPO en de fraudecoördinator).

22 Waaronder bredere implementatie van de praktijk bij Toeslagen van weging van een informatieverzoek om vervolgens bij gerede twijfel een (verder te verwerken) signaal op te voeren.

23 Denk aan opslag in en distributie vanuit datafundamenten ipv handmatig overzetten naar (5+)systemen zoals nu gebeurt.


Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier

bylage 26



Voorafgaand aan het gebruik van gegevens hoort er een toetsing te worden gedaan op de aspecten willen, mogen en kunnen. De WMK-toets zorgt ervoor dat het goede gesprek over deze aspecten kan plaatsvinden door het gestructureerd aflopen van een set relevante items/vragen die door materiedeskundigen onder begeleiding van een WMK-adviseur worden bediscussieerd en vastgelegd.

voor vragen: gegevens@digitaleoverheid.nl

De WMK-toets is op meerdere momenten inzetbaar, in ieder geval in de volgende situaties:

1. Voorafgaande aan een UTNS met een substantiële gegevenscomponent of een PIA (Privacy Impact Assessment). De WMK-toets kan als quick scan worden ingezet om de high-lights van de casus alvast te verkennen en vast te leggen of om te constateren dat een UTNS of PIA (nog) niet zinvol is.
2. Als beoordeling vooraf van een regulier vraagstuk over gegevensgebruik, eventueel als verbijzondering van een lopende UTNS. De WMK-toets wordt ingezet om een over-all beoordeling te geven. De meest voorkomende gebruiksvormen zijn inwinnen, intern doorleveren en verstrekken.
3. Als herijking van een bestaande praktijksituatie van gegevensgebruik.

Uitvoering:

Het sjabloon WMK-toets is in principe geschikt om door betrokken partijen los van elkaar te laten invullen, waarna er centraal verwerking van de deelresultaten tot een totaalbeeld plaatsvindt.

Op basis van ervaringen met inmiddels een dozijn casussen, is vastgesteld dat een sessie met gemandateerde experts van betrokken bedrijfsonderdelen / stakeholders die zich goed hebben voorbereid onder begeleiding van een WMK-adviseur het meest effectief is. Doorgaans is een sessie van 1-1,5 uur voldoende om direct 90+ procent duidelijkheid te verschaffen waarbij tevens de resterende vragen/onderzoekspunten zijn geadresseerd.

VOORBLAD WILLEN-MOGEN-KUNNEN-TOETS	
Inleiding:	De 'Willen, Mogen, Kunnen'-afweging vormt de ruggengraat voor de toetsing die overheden bij het aangaan van een nieuw gebruik van gegevens doen. Elk van deze vragen kent een intern perspectief (wil, mag en kan ik dit voor mijzelf?) en een extern perspectief (hoe pakt de afweging voor mijn omgeving uit?). De 'Willen, Mogen, Kunnen'-afweging vergt betrokkenheid van verschillende bestuurlijke niveaus, schakels in de keten en disciplines. Dat versterkt de noodzaak om een gemeenschappelijk kader te hebben. Dit sjabloon ondersteunt de vastlegging van de bevindingen.
Datum	***donderdag 19 april 2018***
Onderwerp	FSV
Toelichting	
Opdrachtgever	
Uitgevoerd door (WMK-consulent)	
Besproken met (materiedeskundige(n)):	
UTNS?	nvt
Resultaat borgen in:	
Type gegevensverwerking	Intern bewerken
Gegevengebruik al gestart?	
Pilot (J/N)	<onbekend>
Kosten	
Baten	
Bewerkers?	
Gegevens gebruikt voor profiling?	
Toelichting kosten/baten	<>
Extra vragen voor verwerking ten behoeve van analysedoeleinden	
Persoonsgegevens?	
Productkeuze: levering van:	

WILLEN

Intern perspectief			Extern perspectief	
Compliance burger/bedrijf (naleving)			**Moreel acceptabel?**	
Is de (beoogd) opdrachtgever bekend?			Ervaren de betrokkenen dat de rechtszekerheid beter wordt?	
Is er sprake van (meetbare) complianceverbetering?			Ervaren de betrokkenen dat de rechtsgelijkheid beter wordt?	
Past het gegevensgebruik binnen de handhavingsstrategie van het segment?			Is de voorgestelde aanpak maatschappelijk acceptabel?	
Conclusie compliance		B+Gem	*Conclusie Moreel acceptabel?*	
Efficiency			**Verhouding baten/lasten burger en bedrijf.**	
Worden de uitvoeringskosten lager?			Worden de administratieve lasten voor de betrokkenen lager?	
Wordt de doorlooptijd van het proces korter?			Wordt het gebruiksgemak van de producten/diensten verbeterd?	
Is er (zicht op) een positieve business case?			Ervaart de burger/bedrijf een betere dienstverlening?	
Conclusie efficiency		Gem	*Conclusie Verhouding baten/lasten burger en bedrijf.*	
Organisatieontwikkeling			**In lijn met 'hoe de maatschappij werkt'**	
Verbetert de robuustheid van de uitvoering?			Sluit de voorgestelde werkwijze aan bij maatschappelijke ontwikkelingen?	
Is het idee in overeenstemming met de actuele organisatie-inrichtingsplannen?			Voldoet de voorgestelde werkwijze aan hedendaagse standaarden?	
Past de verwerking binnen de IV-architectuur?				
Conclusie organisatieontwikkeling		Gem	*Conclusie In lijn met 'hoe de maatschappij werkt'*	

UITKOMST WILLEN:			
INTERN PERSPECTIEF		UITKOMST:	
	COMPLIANCE		
	EFFICIENCY		
	ORGANISATIEONTWIKKELING		
EXTERN PERSPECTIEF		UITKOMST:	
	MOREEL ACCEPTABEL		
	BATEN / LASTEN		
	HOE MAATSCHAPPIJ WERKT		

OPMERKINGEN&ADVIES:

OPMERKINGEN BIJ INTERN PERSPECTIEF:

Opdr/gever/ eigenaarschap vermoedelijk (inmiddels) impliciet belegd, Persoonsgegevens, Vermogst signalen niet kwantificeerbaar. Eenduidigheid inzet en gebruik niet voldoende geuniformeerd. Door bedrijfsonderdeelgrens overstijgend gebruik mogelijk risico's(FIOD/opsporing, Belastingen (Awr), TSL (Awir))

OPMERKINGEN BIJ EXTERN PERSPECTIEF

Opname in FSV van betrokkenen kent risico van zwarte-lijst(effect) en bv. ongecontroleerde informatiestroom door organisatie; waarde en betekenis van informatie heel divers; doorlevering (RAM?) of eigen extracten door gebruiker naar excel en verder;

Mogen

Intern perspectief			Extern perspectief	
Interne rolverdeling			**Wettelijke grondslag**	
Is de verwerkende (uitvoerende) partij bekend?		<>	Is er een wettelijke grondslag voor de gegevensverwerking?	
Wordt er voorzien in een (aangepaste) procesbeschrijving, AO/IC?			Is de gegevensverwerking proportioneel?	
Wordt er een (interne) leverovereenkomst afgesloten?			De voorgestelde wijze van verwerken is de minst ingrijpende vorm (subsidiariteit).	
			Is de gegevensverwerking noodzakelijk in relatie tot het aantal betrokkenen (burgers/belastingplichtigen)?	
Conclusie Interne rolverdeling		Gem	*Conclusie Wettelijke grondslag*	
Beveiliging			**Doelbinding**	
Voldoet de gegevensuitwisseling aan actuele beveiligingseisen?			Worden de gegevens verzameld voor duidelijk bepaalde doelen?	
Voldoet het toegangs- en autorisatiebeheer aan passende beveiligingseisen.			Is de verdere verwerking verenigbaar met het doel van de oorspronkelijke verwerking?	
Zijn de beveiligingsmaatregelen passend voor de gevoeligheid van de gegevens?			Is de noodzakelijkheid van de verwerking aangetoond (uitvoering publ.rechtelijke taak)?	
			Conclusie Doelbinding	
Conclusie Beveiliging		Gem		
Bewaren, archiveren en vernietigen (BAV)			**Juridische aspecten overig**	
Is het BAV-proces transparant en kenbaar (conform de selectielijsten)?			De gegevensverwerking kan zonder aanbesteding worden geïmplementeerd/uitgevoerd.	
Worden de gegevens niet langer bewaard dan strikt noodzakelijk?			Wordt er een bewerkersovereenkomst of convenant opgesteld?	
Worden de gegevens aantoonbaar vernietigd?			Is beargumenteerd vastgesteld dat er geen PIA wordt uitgevoerd?	
			Conclusie Juridische aspecten overig	
Conclusie Bewaren, archiveren en vernietigen (BAV)		Gem	**Verwijzingen wettelijke grondslag(en)**	
				http://wetten.overheid.nl/BWBR0002320/2016-05-01#HoofdstukVIII_Afdeling2

UITKOMST MOGEN:

INTERN PERSPECTIEF	UITKOMST:
Interne rolverdeling	
Beveiliging	
Bewaren, archiveren en vernietigen (BAV)	

EXTERN PERSPECTIEF	UITKOMST:
Wettelijke grondslag	
Doelbinding	
Juridische aspecten overig	

OPMERKINGEN&ADVIES:

OPMERKINGEN BIJ INTERN PERSPECTIEF:

Teveel mensen hebben toegang; (uit dienst, andere functie, onbekend waarom überhaupt) van bedrijfsonderdelen met een verschillende taak (bv opsporing vs handhaving). IMS profielen bieden toegang tot FSV; voor EOS is dit nader gestructureerd maar dat betreft een beperkt (300-350) deel van de 4400+ gebruikers; bevat bv. ook gebruikers uit begin obv migratie PIT, voorloper FSV ;alle mdw toeslagen werken bv met FSV. Uitgebreid zoeken: ;mdw BI, behandelaar en sr.behandelaar kunnen qua rol bij alle posten; via zoeken algemeen kun je nog steeds heel veel vinden bv door te zoeken op naam of leeglaten zoekcriteria. Logging zou zijn ingeregeld; functioneel bepaald hoe; niet bekend of dit feitelijk is ingericht; idem mbt monitoring; opvoeren nieuwe users via IMS / postbus beheerder FSV; muteren zonder behoud van historie mogelijk; risico; veel oude posten (import pt <2011); verwijderen/vernietigen niet goed functioneel ondersteund (handmatig; ondoenlijk op 550k+ posten). Doorleveren naar RAM; ongeacht soort signaal 'pop' je daar op als je een hit hebt in FSV (fraude, informatieverzoek); 'zwarte lijst'effect" . Onderscheid in raadpleeg rollen; risico is groot aantal users (afgezet tegen karakter verwerkte info/ need to know/kneed to know onderscheid dat beperkt gemaakt kan worden. Té veel incourante users en verouderde info die gearchiveerd / vernietigd had moeten worden.; FSV bevat ook strafrechtelijke info. Risico datalek(ken).

OPMERKINGEN BIJ EXTERN PERSPECTIEF

Verwerkingsdoel(en) te onbepaald icm bij elkaar brengen van veelsoortige categorien gegevens. Zelfs als ieder afzonderlijk verwerkt record een voldoende wettelijke grondslag kent is de bundeling alle verwerkingsdoelen n-op-n koppelbaar (veelal na dump/extract uit FSV). PIA tijdt noodzakelijk. Functionele aanpassingen hieruit voortvloeiend als maatregel op belangrijke deelgebieden al bekend/beschreven en ten dele ook geprioriteerd.

Kunnen

Intern perspectief			Extern perspectief		
Maakbaarheid			**Maakbaarheid**		
Sluit de verwerking aan bij de kanalenstrategie?			Kan de verwerking worden gerealiseerd met e-overheidsvoorzieningen?		
Kan de verwerking worden gerealiseerd met bestaande IV-voorzieningen?			Kan de verwerking worden gerealiseerd met marktvoorzieningen?		
Kan de verwerking worden gerealiseerd met innovatie IV-voorzieningen?					
			Conclusie externe Maakbaarheid		Gem
Conclusie Maakbaarheid		Gem	**Realiseerbaarheid**		
Realiseerbaarheid			Zijn de gegevens bruikbaar?		
Is er budget en gekwalificeerd personeel beschikbaar voor de realisatie?			Zijn de gegevens tijdig beschikbaar?		
Kan het project worden ingepland binnen het ontwikkelportfolio?					
Is de kwaliteit van de gegevens als voldoende (vastgesteld) voor verwerking?			*Conclusie externe Realiseerbaarheid*		Gem
Conclusie Realiseerbaarheid		Gem	**Correctie en inzagerecht**		
Implementeerbaarheid			Bestaat er een (vindbare /toegankelijke) inzagevoorziening?		
Zijn er duidelijke acceptatiecriteria vastgesteld en geaccepteerd?			Bestaat er een (vindbare /toegankelijke) correctievoorziening?		
Past de gegevensverwerking binnen de bestaande formatie/bezetting?			*Conclusie Correctie en inzagerecht*		Gem
Past de gegevensverwerking binnen de bestaande processen/werkwijze?			**Implementeerbaarheid**		
Conclusie Implementeerbaarheid		Gem	Zijn er duidelijke acceptatiecriteria vastgesteld en geaccepteerd?		
			Zijn eventuele externe producten en diensten tijdig beschikbaar?		
			Conclusie externe Implementeerbaarheid		Gem

UITKOMST KUNNEN:

OPMERKINGEN&ADVIES:

INTERN PERSPECTIEF		UITKOMST:
	Maakbaarheid	
	Realiseerbaarheid	
	Implementeerbaarheid	

OPMERKINGEN BIJ INTERN PERSPECTIEF:

FSV in beheer/onderhoud bij LIV; browser-based; opgenomen in iMS maar geen product reguliere IV-keten. Er zijn geprioriteerde must en should do gebruikerseisen en wensen; realisatiekans / moment onbekend. Datakwaliteit heel divers ; deels inherent aan type info (kliks) deels afhankelijk van actualiteit, wijze verwerking. Bij juist gebruik mogelijk voldoende maar risicovol bij onjuist gebruik.

EXTERN PERSPECTIEF		UITKOMST:
	Maakbaarheid	
	Realiseerbaarheid	
	Correctie en inzagerecht	
	Implementeerbaarheid	

OPMERKINGEN BIJ EXTERN PERSPECTIEF

Inzage/correctierecht van toepassing en zo ja is daar dan in voorzien?

FSV

Advies

	INTERN PERSPECTIEF	Opmerkingen	EXTERN PERSPECTIEF	Opmerkingen
Willen	Compliance burger/bedrijf (naleving)	Opdr/gever/ algenaarschap vermoedelijk (inmiddels) impliciet bekend. Persoonsgegevens Opbrengst signalen niet kwantificeerbaar. Eenduidigheid inzet en gebruik niet voldoende geuniformeerd. Door bedrijfsonderdeelgrens overstijgend gebruik mogelijk risico's(FIOD/opsporing, Belastingen (Awr), TSL (Awir))	Moreel acceptabel?	Opname in FSV van betrokkenen kent risico van zwarte-lijst(effect) en bv. ongecontroleerde informatiestroom door organisatie; waarde en betekenis van informatie heel divers; doorlevering (RAM?) of eigen extracten door gebruiker naar excel en verder;
	Efficiency		Verhouding baten/lasten burger en bedrijf.	
	Organisatieontwikkeling		In lijn met 'hoe de maatschappij werkt'	
	INTERN PERSPECTIEF		**EXTERN PERSPECTIEF**	
Mogen	Interne rolverdeling	Teveel mensen hebben toegang; (uit dienst, andere functie, onbekend waarom überhaupt) van bedrijfsonderdelen met een verschillende taak (bv opsporing vs handhaving). IMS profielen bieden toegang tot FSV; voor EOS is dit nader gestructureerd maar dat betreft een beperkt (300-350) deel van de 4400+ gebruikers; bevat bv. ook gebruikers uit begin obv migratie PIT, voorloper FSV ;alle mdw toeslagen werken bv met FSV. Uitgebreid zoeken: ;mdw BI, behandelaar en sr.behandelaar kunnen qua rol bij alle posten; via zoeken algemeen kun je nog steeds heel veel vinden bv door te zoeken op naam of leeglaten zoekcriteria. Logging zou zijn ingeregeld; functioneel bepaald hoe; niet bekend of dit feitelijk is ingericht; idem mbt monitoring; opvoeren nieuwe users via IMS / postbus beheerder FSV; muteren zonder behoud van historie mogelijk; risico; veel oude posten (import pit <2011); verwijderen/vernietigen niet goed functioneel ondersteund (handmatig; ondoenlijk op 550k+ posten). Doorleveren naar RAM; ongeacht soort signaal 'pop' je daar op als je een hit hebt in FSV (fraude, informatieverzoek); 'zwarte lijst'effect" . Onderscheid in raadpleeg rollen; isico is groot aantal users (afgezet tegen karakter verwerkte info/ need to know/kneed to know onderscheid dat beperkt gemaakt kan worden. Te veel incourante users en verouderde info die gearchiveerd /vernietigd had moeten worden ; FSV bevat	Wettelijke grondslag	Verwerkingsdoel(en) te onbepaald icm bij elkaar brengen van veelsoortige categorien gegevens. Zelfs als ieder afzonderlijk verwerkt record een voldoende wettelijke grondslag kent is de bundeling alle verwerkingsdoelen n-op-n koppelbaar (veelal na dump/extract uit FSV). PIA lijkt noodzakelijk. Functionele aanpassingen hieruit voortvloeiend als maatregel op belangrijke deelgebieden al bekend/beschreven en ten dele ook geprioriteerd.
	Beveiliging		Doelbinding	
	Bewaren, archiveren en vernietigen (BAV)		Juridische aspecten overig	
	INTERN PERSPECTIEF		**EXTERN PERSPECTIEF**	
Kunnen	Maakbaarheid	FSV in beheer/onderhoud bij LIV; browser-based; opgenomen in IMS maar geen product reguliere IV-keten. Er zijn geprioriteerde must en should do gebruikerseisen en wensen; realisatiekans / moment onbekend. Datakwaliteit heel divers ; deels inherent aan type info (kliks) deels afhankelijk van actualiteit, wijze verwerking. Bij juist gebruik mogelijk voldoende maar risicovol bij onjuist gebruik.	Maakbaarheid	Inzage/correctierecht van toepassing en zo ja is daar dan in voorzien?
	Realiseerbaarheid		Realiseerbaarheid	
	Implementeerbaarheid		Correctie en inzagerecht	
			Implementeerbaarheid	

Blokkerende bevindingen

	De wettelijke grondslag ontbreekt of is niet aangetoond.	1
	De geheimhoudingplicht wordt geschonden.	2

Minst optimaal

Productkeuze;levering van	Persoonsgegevens	Pseudoniem	Anoniem
Data van alle subjecten			
Selectie van de subjecten			
Een geaggregeerde data-set			
Een gecategoriseerde data-set			
Een gegevensproduct; direct antwoord op procesvraag			

Meest optimaal

	Procedurele signalen	
1	Vul het Voorblad (verder) in.	
2		
3		
4		
5		

	Inhoudelijke signalen	
1		
2		
3		
4	Nog geen oordeel mogelijk over realiseerbaarheid.	
5		
6		
7		
8		
9		
10	Voer een PIA of privacy audit uit.	

	Mini-Business Case (kosten/baten)
Kosten	0
Baten	0
Toelichting kosten/baten	<>

tabblad Beheer

Grenswaarden	TypeGegGebruik	J/N vragen	Onbekend	Prioriteit stellen	Beveiligingsnormen	Persoonsgegevens	
0	Inwinnen	Ja	Gegevensvraag	Levertijd 8 wkn	HBB	Pseudoniem	Selectie van de subjecten
1	Verstrekken	Nee	ZGO	Cfrm aanvraag	VIR	Anoniem	Een geagregeerde data-set
2	Intern bewerken	Ja R&D	MKB		ISO 270001/2		Een gecategoriseerde data-set
3	<onbekend>	<onbekend>	PDB				Een gegevensproduct, direct antwoord op procesvraag
7							

Data van alle subjec Waardetabellen die op een aantal pagina's als dropdowi

Tellingen	Dashboard=
0	0
2	1
7	2
3	3
3	7
Gem	2,083333

n lijstjes beschikbaar zijn

Fixes in .99 versie

1 Nieuwe blokkerende bevinding: als verstrekken=ja en geheimhouding doorbroken =nee
2 Gemiddelden worden berekend zonder NVT en leeg waarde
3 Invoer antwoord uitgebreid naar 1=Ja=(groen); 2=twijfel/riskant (oranje); 3=nee (rood)
4 Tekstuele verbeteringen vragen mogen;extern
5 Werkbladen beveiligd

voor vragen: gegevens@digitaleoverheid.nl

bylage 27

Belastingdienst

VERTROUWELIJK

memo

Besluitenlijst MT MKB
Utrecht

Midden- en kleinbedrijf
MT
Korte Voorhout 7
2511 CW Den Haag
www.belastingdienst.nl

Persoonsgegevens

Besluitenlijst van 30 april (Rotterdam), 7 mei (Utrecht) en 14 mei 2018 (Rotterdam)

Afwezig: Persoonsgegevens (30 april)
7 mei: laatste MT-vergadering Persoonsgegevens

Datum
14 mei 2018

Vastgesteld door
MT

Auteur
Persoonsgegevens

Kopie aan
Medezeggenschap

Bijlagen
1

1. Ontwikkelagenda MKB
Het MT MKB bespreekt de voortgang van de Ontwikkelagenda MKB. Men neemt kennis van een globale samenvatting van de uitwerking per focuspunt. Op de MT-heidag van 16 en 17 mei zal de concept-Ontwikkelagenda worden besproken. Het MT stemt in met de bespreekpunten voor de heisessie, zoals traject na juni en Communicatie en de planning zoals die er ligt, met een gateway review in de week van 11-15 juni.

2. Informatieloketten
Te gast Persoonsgegevens om het onderwerp informatieloketten toe te lichten. De bij de 11 informatieloketten binnen de specialteam Fraude/EOS uitgevoerde Gegevensbeschermingseffectbeoordeling (=PIA) inventariseert risico's en issues met betrekking tot de privacybescherming en doet aanbevelingen om deze te reduceren. Het MT MKB neemt kennis van het rapport en keurt deze goed. Goedkeuring door het MT leidt ertoe dat aan de door het programma AVG geformuleerde basispositie rondom invoering van de AVG is voldaan. Van belang is daarbij dat de basis voor de gegevensverwerking binnen de informatieloketten goed is. In het rapport zijn risico's en maatregelen rondom adequate bescherming van de privacy in kaart gebracht:
- Het MT verzoekt te inventariseren wat er omtrent dit aspect bij de SFO's speelt en deze te delen met de stuurgroep Huisvesting.
- Het MT MKB geeft verder aan dat de bevindingen uit de nog uit te voeren WMK-toets op FSV opgepakt moeten worden.
- Conform de aanbevelingen gaat het MT MKB akkoord met de formatie van een werkgroep met de opdracht de aanbevelingen rondom uniformering en centrale aansturing uit te werken in landelijke werkinstructies en datasets. Daarbij dient er borging te zijn met het MT en de data officer.
- Het MT MKB gaat akkoord met het voorstel om het vraagstuk van de brede informatiestromen ter hand te nemen conform het op 2 juni 2017 door het toenmalige CDO2 genomen besluit. Dit wordt opgepakt door het al bestaande Brede Informatiestromen Overleg (BIO) een (nader) vooronderzoek te laten uitvoeren als opstap voor een vervolg in lijn met dit besluit.
- Het MT MKB geeft aan LC F/EOS te laten bewaken dat RIEC-IS wat inhoud, gebruik en toegang betreft voldoet of gaat voldoen aan de AVG.

@Stuk wordt verspreid aan plv. directeuren.

3. Summarische Risiko Prufung (SRP)
In Duitsland wordt voor de beoordeling van de volledigheid van de omzet bij ondernemingen onder andere gebruik gemaakt van de tool Summarische Risiko Prüfung (hierna: SRP). In opdracht van het Management MKB en in samenwerking met landelijk Vaktechniek Controle en Formeel recht is vanaf 2016 in een pilot de bruikbaarheid van de SRP bij boekenonderzoeken in het segment MKB onderzocht. Het MT MKB

neemt kennis van de eindevaluatie. Gezien de bevindingen in de eindevaluatie stemt het MT MKB met een vervolg aan het gebruik van deze gratis tool. Het vervolgt ziet toe op de activiteiten uit het werkplan. Dat betekent in ieder geval binnen de horeca en zo mogelijk voor andere branches bij posten uit de Steekproef ondernemingen of indien mogelijk bijvoorbeeld binnen de autohandel. Het gebruik wordt daarbij uitgebreid naar een locatie per verzorgingsgebied. In overleg met Vaktechniek zal er aandacht worden besteed aan het onderwerp 'administratieplicht.' Het MT MKB vindt het van belang dat eea wl goed gemonitord kan worden. Hoe deze tool geformaliseerd kan worden, zodat het onderhoud en beheer is gegarandeerd, dient verkend te worden met de data officer.

4. PvA Horecea
Eerder is de aanpak Horeca 2018 – 2020 aan de orde geweest. Het MT MKB heeft ingestemd met het voorstel voor een brede aanpak horeca (in drie sporen) en heeft opdracht gegeven de voorgestelde richting verder uit te werken, inclusief planning.
Het MT MKB stemt nu in met het plan van aanpak, dat tot stand is gekomen met EHI. Het plan zal ter informatie ook naar de directie UHB worden gestuurd.

5. Evaluatie Goudhandel
Het MT MKB neemt kennis van het evaluatierapport Goudhandel. Eind 2016 is op advies van EHI en de FIOD met een pilot Goudhandel op 3 MKB-kantoren gestart. De focus ligt op bedrijven die zich nagenoeg uitsluitend bezighouden met de in- en verkoop van tweedehands goud.
Het MT MKB in het met het voorstel om:
- Een vervolgaanpak van de goudhandel te positioneren binnen 4 RIEC's (Rotterdam, Den Haag, Oost-Nederland en Noord)
- Detectie en selectie te laten plaatsvinden binnen de genoemde RIEC's
- De verantwoordelijkheid voor het vervolg binnen de Belastingdienst onder de verantwoordelijkheid van de landelijk coördinatie EOS/Fraude te positioneren.

6. Forum salaris
Het MT MKB stemt in met het voorstel om het Forum Salaris als special binnen MKB Eindhoven voort te zetten. Forum Salaris is in april 2016 binnen MKB van start gegaan als pilot. De inzet is om samen met de doelgroep salarisadministrateurs te werken aan een betere loonaangifte. Dit met als doel de verbetering van de kwaliteit van gegevens in de polisadministratie. Sprake is inmiddels van stabiele routines, waarbij steeds meer synergievoordelen worden behaald in de samenwerking met Forum Fiscaal Dienstverleners. In dat kader stemt het MT MKB in met het voorgenomen besluit om het combineren van het Forum FD en Forum Salaris in een nieuwe landelijke special, genaamd special FORA-team, gekoppeld aan MKB Eindhoven. Dit betekent dat het MT MKB ook instemt met toekenning van een budget van 15.000 euro voor out-of-pocketkosten en de huidige capaciteit van 8,8 fte MKB-medewerkers hieraan te blijven verbinden. Het MT MKB geeft wel mee als aandachtspunt dat er verbinding moet zijn met de Ontwikkelagenda en keten.

7. MKB in Beeld
De tweede reeks van de filmpjes 'MKB in Beeld' is in volle gang. De edities over 'belastingtoezicht naar de voorkant' en 'blockchain' zijn reeds uitgekomen. Inmiddels is echter sprake van een aantal nieuwe ontwikkelingen, die bijstelling van de geplande reeks onderwerpen wenselijk/noodzakelijk maakt. Het MT MKB gaat akkoord met de onderwerpen, 'Ondernemers onder toezicht, hoe doen we dat?' en 'Toezicht Internationaal'.

8. Rapportage HIA/IA

Het MT MKB stemt in met de rapportage HIA/IA die – na appreciatie van DO Control – wordt aangeboden aan Bureau Investeringsagenda (BIA).

9. Handhavingsplan ANBI
In het handhavingsplan geeft het ANBI-team inzicht waar het team voor staat en welke afwegingen gemaakt moeten worden over de inzet van capaciteit. Omdat het ANBI-team segmentoverstijgende activiteiten verricht is dit handhavingsplan onder leiding van P en in samenwerking met MKB, GO, EHI en Communicatie tot stand gekomen. Het MT MKB gaat akkoord met het plan. Het handhavingsplan zal voor het driehoeksoverleg UHB/.FJZ worden geagendeerd.

10. Bijzonder belonen 2018
In het DT BD van 15 januari is het budget bijzonder belonen 2018 vrij gegeven. Het MT MKB stemt in met de werkinstructie voor tav dit onderwerp. In de notitie wordt
Met betrekking tot het individueel bijzonder belonen van MKB medewerkers, zal er een voorstel in de nazomer worden aangeboden. Vooruitlopend op dit voorstel, wordt in deze notitie voor de Belastingdienst eenheid van (uitvoering van) beleid uiteengezet en wordt een bijdrage geleverd aan de beheersing van onder andere financiële en fiscale risico's (regelgeving Loonheffingen). @De notitie wordt verspreid aan plv. directeuren.

bylage 28

Item 26:
In de allereerste versie van de GEB (v.0.1) stond een concept-opsomming op attribuutniveau. Vanaf versie 0.2 is dit gewijzigd in een categoriegewijze opsomming zoals gevraagd in het Rijksmodel PIA. Aanvankelijk was het idee om de uitgebreide opsomming integraal op te nemen als bijlage. Verderop in het proces is gekozen (zonder duidelijk/reconstrueerbaar beslismoment) om daar van af te zien echter abusievelijk zonder verwijdering van de verwijzing naar de bijlage. Hieronder is de opsomming uit de 0.1-versie weergegeven.

Tekst GEB v. 0.1 dd 20181106 (met kleuren zoals in oorspronkelijk document aanwezig overgenomen)	**Type**
Persoonsgegeven	
BSN	Wettelijk identificerend
Achternaam	Gewoon
Voorletters	Gewoon
Voorvoegsels	Gewoon
Soort fraude	?
Middel	
Belastingjaar	
Prioriteit	'Zwarte lijst'?
Adres	Gewoon
Postcode	Gewoon
Plaats	Gewoon
Land	Bijzonder
Kwalificatie als:	
Dader:	Strafrechtelijk
Geen dader:	Strafrechtelijk
Geen slachtoffer:	Strafrechtelijk
Mededader:	Strafrechtelijk
Medeplichtige:	Strafrechtelijk
Onbekend:	Strafrechtelijk
Slachtoffer:	Strafrechtelijk
Besmet adres:	'Zwarte lijst'?
Besmet postcode en nr.	'Zwarte lijst'?
Belastingjaar	
Rekeningnummer	Gewoon
Negatieve norm OB	'Zwarte lijst'?
Bron	?
IP-adres	Gewoon
MAC-adres	Gewoon
Prioriteit	Zwarte lijst
Aangiftefraude: (Rechterzijde tabblad):	Strafrechtelijk
Datum opname:	Strafrechtelijk
Datum afdoening:	Strafrechtelijk
Correctiebedrag:	Gewoon
Fiscaal nadeel:	Gewoon
Belastingbedrag:	Gewoon
Boete	Bestuurlijke boete?
Boetebedrag	Bestuurlijke boete?
Boetepercentage	Bestuurlijke boete?
Strafrechtelijke beschikking	Strafrechtelijk
Aangemeld bij FIOD	Strafrechtelijk

Fraude	Strafrechtelijk
ID-fraude	Strafrechtelijk
Gefisnummer	Strafrechtelijk
Beconnummer	Gewoon
Fiscaal dienstverlener BSN:	Wettelijk identificerend
Fiscaal dienstverlener naam	Gewoon
Inhoudingsplichtige LH nr.:	Gewoon
Inhoudingsplichtige LH naam:	Gewoon
Opgevoerd door:	Gewoon
Beoordeeld door:	Gewoon
Behandeld door:	Gewoon
Partner BSN:	Wettelijk identificerend
Partner naam:	Gewoon
LRK:	Wettelijk identificerend
Invordering:	
Projectcode landelijk	
Aantekeningen	

bijlage 2g

Feature naam	Aanpassingen FSV
Feature code	F18.045
Versie	0.5
Datum	22-10-2018
Hoort bij Epic	E16.321
Business	Persoonsgegevens
Auteur	Persoonsgegevens
Architect	Persoonsgegevens

Korte Omschrijving (Max 5 regels)
De applicatie Dagboek FSV (Fraude Signalering Voorziening) is bestemd voor de registratie van fraudesignalen. Primair voor signalen van systeemfraude voor meerdere belastingmiddelen en verschillende Toeslagen. Daarnaast kan de applicatie ook gebruikt worden voor de registratie van tips/kliks/signalen, projecten (per segment, regionaal, plaatselijk) in het Subject Gerichte Toezicht en voor de registratie van bijzondere verzoeken om informatie, misbruik van bijstandsuitkeringen, RIEC verzoeken, enzovoort. Door het vastleggen van deze gegevens, kunnen over een bepaalde periode wellicht bepaalde trends in beeld worden gebracht, bestuurlijke informatie worden verstrekt, en mogelijke andere relevante informatie worden verzameld.

Requirements
Als medewerker van de MKB fraudeteams/EOS, de PDB fraudeteams en het Toeslagen fraudeteam wil men dat in de Dagboek FSV een aantal aanpassingen worden doorgevoerd zodat de applicatie voldoet aan de per 25 mei 2018 van kracht geworden verordening AVG.
Op 6 november 2018 wordt er in dit kader een PIA (Privacy Impact Assessment) waarin de gevolgen van deze regelgeving voor FSV worden bekeken.
Verder zijn er een aantal wensen/aanpassingen beschreven die het gebruik van de applicatie zullen verbeteren/vereenvoudigen zodat de kansen op onjuiste informatie verminderd. Ook resulteert dit in betere en betrouwbaardere BI over deze signalen.

Mogelijke oplossingsrichting
Zie hiervoor onder 'Uitwerking'.

Uitgangspunten, ontwerpbeslissingen en besluiten
Uitgangspunt is dat de gebruikers van de applicatie Dagboek FSV ook na de wetswijziging een juiste tool hebben om hun gegevens in vast te leggen en later weer te kunnen produceren.
Door het besluit van het MT MKB (24-05-2017) wordt het gebruik van de applicatie Dagboek FSV steeds belangrijker en is sindsdien verplicht gesteld voor MKB.

Raakvlakken:
Anti Fraude Box / Toeslagen

Uitwerking
De gevraagde aanpassingen voor de applicatie heb ik hieronder beschreven.

1. Archieffunctie.

Door het steeds intensiever gebruik maar ook gelet op de regelgeving uit bijvoorbeeld de archiefwet, is het gewenst dat oudere signalen worden gearchiveerd. Thans ontbreekt hiertoe de mogelijkheid. Verwezen wordt in dit kader naar de Algemene Verordening Gegevensbescherming welke vanaf 25 mei 2018 van toepassing wordt.
I.v.m. de genoemde wettelijke voorschriften en de Archiefwet 1995 is het nodig dat oudere signalen worden gearchiveerd en elders worden opgeslagen. Op grond van diezelfde wettelijke voorschriften moeten ze wel raadpleegbaar blijven.
Het gaat i.c. om zowel de data (signalen zoals deze zijn opgenomen in FSV) als de bijlagen welke bij deze data zijn opgeslagen.

Voorstel: Wanneer een zaak/signaal klaar is wordt de datum afdoening ingevuld.
De zaak/het signaal waarvan de datum afdoening is ingevuld moet dan naar het archief.
In het archief zijn zaken nog wel raadpleegbaar maar niet meer muteerbaar. Vanaf dan zijn de wettelijke termijnen van toepassing van AVG en de Archiefwet en moet er na die wettelijke termijn (meestal 7 jaar, nog uitzoeken in selectielijst) geschoond. Wanneer er geschoond wordt, dan worden de gegevens weggegooid. Dit zal jaarlijks conform de voorgeschreven termijnen dienen te gebeuren. Het raadplegen van de gearchiveerde data wordt beperkt voor de gebruikers met de rol van 'senior-behandelaar'
Afgestemd met de gebruiker is in dit voorstel dat hij er voor zorg draagt dat signalen die afgedaan zijn en om wat voor reden dan ook niet van een einddatum (datum afdoening) zijn voorzien bijvoorbeeld in een 'massaal' proces van een einddatum worden voorzien. Vervolgens kan daarna het normale proces van archivering in gang gezet worden.
De bijlagen, lees documenten, die bij een signaal horen moeten worden gearchiveerd in ARC.

2. Verwijderen van regels in uitklapbare keuzemenu's (dropdownlists)

Bij het onderdeel 'Informatieverzoeken' worden in diverse uitklapbare keuzemenu's 'z', '..', '—' of 'x' of anderszins notities gemaakt, omdat er geen regels kunnen worden verwijderd (De beheerder kan wel regels toevoegen en wijzigen). Dit werkt het maken van fouten in de hand en is vervuilend voor het bestand van FSV. In een aantal gevallen worden dit soort 'notities' gebruikt bij het opslaan van signalen. Dit is onjuist en geeft verkeerde informatie bij overzichten. Daarnaast werkt dit het 'niet gebruiken van FSV' in de hand. Door deze werkwijze zijn de keuzemenu's in de loop van de tijd erg groot geworden. Ten gevolge van het grote aantal mogelijkheden, ontbreekt het overzicht en worden signalen niet juist geboekt in FSV op dit moment. Gevraagd wordt om menu-items te verwijderen.
De volgende oplossing wordt voorgesteld;
Voor gebruikers met de rol van 'beheerder' moet het beheer uitgebreid worden met de mogelijkheid om regels uit de uitklapbare keuzemenu's uit te schakelen door menu-items middels het invullen van een vervaldatum te deactiveren. De regels zijn dan niet meer benaderbaar.
De gebruiker heeft er geen behoefte aan om die menu-items en de eventueel daar bij gemaakte notities nog te bewaren en compleet verwijderen is geen probleem.

3. Update maken (dump) van database FSV.

Zowel de data analisten van CA (AFB), EHI als de invordering willen direct / rechtstreeks toegang hebben tot de database FSV c.q. hier een (complete) dump van kunnen maken. Alle gegevens welke in FSV zijn opgenomen zijn van belang voor analyse met andere beschikbare gegevens binnen de Belastingdienst. Hierdoor ontstaat de mogelijkheid om (nog meer) gericht werkwijze, methodes, preventief en repressief te ontwikkelen t.b.v. misbruik van fiscale regelgeving.
Door het steeds meer werken met beschikbare informatie kunnen de juiste keuzes worden gemaakt op basis van alle beschikbare gegevens.
Voor de invordering zijn deze gegevens van belang om op een juiste en passende wijze de subjecten te kunnen beoordelen voor "stickering" van de als fraude aangemerkte signalen in de Debiteuren administratie INL (1X1 teams). Dit ter voorkoming dat deze debiteuren ten onrechte in aanmerking komen voor kwijtschelding (IH) c.q. niet verder bemoeilijken voor Toeslagen. Ook de signalering als fraudepost in de 1X1 teams voorkomt instemming / toelating tot de schuldsanering (MSNP/WSNP).

De regiearchitect heeft over dit onderwerp het volgende gezegd;
'We willen af van de datadumping mogelijkheden (mag niet n.a.v. AVG beleid). N.a.v de RAM uitfasering wordt gewerkt aan de vervanging van (onder meer) RAM - de Intelligence Voorziening Toezicht. Als onderdeel van die voorziening is ook het aanvraagproces (doelbinding etc) conform AVG ingericht.
Ihkv IVT en vervolg wordt gewerkt aan de invulling van portfoliowerk voor de komende jaren. Daarin is ook onderkend dat er bronnen en gegevens toegevoegd zullen moeten worden aan IVT.

En er zal meegewogen moeten worden in hoeverre fraudesignaleringen kunnen worden toegevoegd.'
Dit onderwerp zal m.n. op 6 november 2018 tijdens de PIA sessie onderwerp van gesprek zijn.

4. Wijziging namen door userid.

Het aantal medewerkers wat is (en wordt) geautoriseerd voor dagboek FSV loopt op. Hierbij gebeurd het dat medewerkers onder verschillende namen meerdere malen worden opgevoerd als geautoriseerde medewerker. Dit geeft vervuiling en onjuiste info over het werk van die medewerkers. Het gebruik van userid is uniek en eenvoudiger.
De gebruiker wil medewerkers in FSV op voeren met hun userid. Van de medewerker worden de volgende zaken vastgelegd, userid, naam, Sap nummer en competente eenheid. Dit gebeurd nu handmatig wat de uiteraard de kans op fouten vergroot.
Om dit realiseren worden 2 voorstellen gedaan. De eerste variant is een controle maken dat een userid en een SAP nummer maar 1 maal ingevoerd kan worden en niet in verschillende combinaties.
Een andere oplossing is om een tabel toe te voegen waarbij bij het opvoeren van het userid de overige 3 velden automatisch gevuld worden.
In beide gevallen is een unieke vastlegging van de medewerker met userid en Sap nummer gewaarborgd. In het laatste geval is een unieke vastlegging van userid, naam, SAP nummer en competente eenheid gewaarborgd.
Gebruiker wil wel dat de thans aanwezige signalen wel raadpleegbaar blijven.
Aansluitend wil de gebruiker het zoeken op naam in de invoervelden 'beoordeeld door' en 'behandeld door' wijzigen in zoeken op userid. Dit gaat sneller en vele malen accurater.
Aangezien niet in alle gevallen het userid bekend is lijkt het wenselijk om de standaard zoek optie te wijzigen in userid en daarnaast het zoeken op naam in stand te laten.
Op de volgende plaatsen in de applicatie komen de bedoelde gegevens voor:
Zowel bij opvoer als raadplegen zijn er drie rubrieken waar de namen voorkomen:

1) "Opgevoerd door"
2) "Beoordeeld door"
3) "Behandeld door"

Bij de functie "mijn openstaande posten", wordt alleen gezocht op de posten die op "mijn naam" open staan als "beoordeeld door" en "behandelaar".
Bij functie "raadplegen" kan alleen gezocht worden op "behandelaar".

5. Verbandscontrole / automatisch naar volgende rubriek. (tabblad aangiftefraude)

Dit onderdeel is met het bouwteam besproken en aangezien deze functionaliteit inbouwen erg arbeidsintensief is en dat een juiste werking daarna nog maar de vraag is wordt dit verzoek door de gebruiker als heel laag geprioriteerd en tot nader order geparkeerd.

In het tabblad aangiftefraude moeten veel gegevens worden geregistreerd. Dit is een arbeidsintensief traject. Om dit traject te versnellen wordt voorgesteld om een aantal rubrieken 'automatisch' (d.m.v. bijv. tabtoets) te laten passeren om in te vullen.
Het idee hierbij is dat er in de achtereenvolgende invoervelden een bepaalde logische volgorde zit en dat de cursor met de tabtoets naar het volgende veld te laten springen.
Die logische volgorde voor het tabblad 'Aangiftefraude' is hieronder aangegeven.
(Voor de andere tabbladen is geen aanpassing nodig, daar kan de normale manier van met de Tab toets springen naar het eerst volgende veld gehandhaafd blijven)

Aangiftefraude: (Linkerzijde tabblad):

BSN	tab toets naar
Achternaam	tab toets naar
Voorletters	tab toets naar
Voorvoegsels	tab toets naar
Soort fraude	afhankelijk van de keuze die hier gemaakt wordt, kun je dan met de tabtoets naar de juiste rubriek gaan. Dit is op afhankelijk van de mogelijkheden op de afrolmenu's

	Fraude aangaande Toeslagen: rubrieken: - middel - Belastingjaar - Prioriteit
Adres	tab toets naar
Postcode	tab toets naar
Plaats	tab toets naar
Land	tab toets naar
Rol	afhankelijk van de keuze die hier gemaakt wordt, kun je dan met de tabtoets naar de juiste rubriek gaan. Dader: zoveel mogelijk volgende rubrieken van belang Geen dader: idem Geen slachtoffer: idem Mededader: idem Medeplichtige: idem Onbekend: idem Slachtoffer: idem
Besmet adres:	tab toets naar
Besmet postcode en nr.	tab toets naar
Middel	afhankelijk van de keuze die hier gemaakt wordt, kun je dan met de tabtoets naar de juiste rubriek gaan: Middel: toeslagen gerelateerd, dan is rubriek 'subnummer' en 'tijdvak' niet van belang IH: rubriek 'jaar' van belang LH: rubriek 'belastingjaar', 'subnummer', en 'tijdvak' van belang OB: rubriek 'belastingjaar', 'subnummer', 'tijdvak' en 'negatieve norm OB' van belang
Belastingjaar	tab toets naar
Rekeningnummer	tab toets naar
Negatieve norm OB	tab toets naar
Bron	tab toets naar
IP-adres	tab toets naar
MAC-adres	tab toets naar
Prioriteit	in principe alleen van belang voor Toeslagen

Aangiftefraude: (Rechterzijde tabblad):

Datum opname:	tab toets naar
Datum afdoening:	tab toets naar
Correctiebedrag:	verplicht veld bij datum afdoening
Fiscaal nadeel:	verplicht veld bij datum afdoening
Belastingbedrag:	verplicht veld bij datum afdoening
Boete	tab toets naar
Boetebedrag	verplicht veld bij invullen rubriek 'boete'
Boetepercentage	verplicht veld bij invullen rubriek 'boete'
Strafrechtelijke beschikking	tab toets naar
Aangemeld bij FIOD	tab toets naar Gefisnummer
Fraude	tab toets naar
ID-fraude	tab toets naar
Gefisnummer	tab toets naar
Beconnummer	tab toets naar
Fiscaal dienstverlener BSN:	tab toets naar
Fiscaal dienstverlener naam	tab toets naar
Inhoudingsplichtige LH nr.:	tab toets naar
Inhoudingsplichtige LH naam:	tab toets naar
Opgevoerd door:	tab toets naar
Beoordeeld door:	tab toets naar
Behandeld door:	tab toets naar

Competente eenheid:	tab toets naar
Partner BSN:	tab toets naar
Partner naam:	tab toets naar
LRK:	Afhankelijk van keuze bij middel 'Toeslagen". Indien sprake van KOT dan LRK invullen
Invordering:	tab toets naar
Projectcode landelijk	tab toets naar
Aantekeningen	tab toets naar

Afsluitende rubrieken "opslaan" – "Annuleren".

6. Zoeken op woord, tekst over alle tabbladen heen (met name ook in rubriek aantekeningen).

In de praktijk komt het voor dat men wel weet over wie of wat het gaat, maar het BSN of dossiernummer is onbekend of het is onduidelijk waar het signaal is opgenomen of onder welke noemer het is opgenomen. Door bij "overzichten" de mogelijkheid te maken om te zoeken op een tekstgedeelte kan nog beter gebruik worden gemaakt van FSV wat de registratie van signalen en daardoor het inzicht in fraude(patronen) nog meer duidelijkheid geeft.
Het volgende wordt voorgesteld;
Wanneer je wilt zoeken in open velden gaat dat ten koste van de performance. Laat daarom de huidige zoekfunctie bestaan voor de gebruikers. Bouw vervolgens daarnaast een (extra) zoekfunctionaliteit zoals gewenst maar geeft die optie alleen aan gebruikers met de rol van 'Senior behandelaar'.

7. Massaal verwijderen signalen

Dit onderdeel is met het bouwteam besproken en aangezien de business nog niet helder heeft welke criteria er zijn om dubbelingen te herkennen wordt dit verzoek door de gebruiker als heel laag geprioriteerd en tot nader order geparkeerd.

Helaas komt het voor dat bij het massaal inlezen van signalen vergissingen worden gemaakt, of signalen anderszins hadden moeten worden opgenomen. Bij het dagboek PIT konden deze 'in een keer' door de beheerder worden verwijderd. Deze mogelijkheid ontbreekt thans. Hierdoor zijn er in een aantal gevallen signalen nog dubbel opgenomen. In de meeste gevallen zijn deze stuk voor stuk verwijderd wat erg arbeidsintensief is (geweest).
Er drie mogelijkheden voor massaal inlezen: aangiftefraude, bijwerken aangiftefraude en project/overig. De wens is om dan één van deze specifieke items over een bepaalde periode weer kunnen verwijderen als beheerder.
Verder ook gegevens welke in een bepaalde periode (tijdvak) zijn ingeboekt of afgedaan. Bijvoorbeeld: Alle (dus van alle tabbladen) gegevens welke zijn ingevoerd in een periode (01-01-1990 t/m 31-12-2000) moeten allen worden verwijderd in verband met archiefwetgeving. De bedoeling is dan dat deze dan 'in een keer' massaal kunnen worden verwijderd (gearchiveerd).

8. Bericht zenden (mail) aan alle geautoriseerde medewerkers. Vervallen

Risico's

Integriteit	Wanneer er geen aanpassing wordt gedaan aan de ontsluiting via Excel kan niet worden ingestaan voor de gegevens in FSV.
Performance	Deze applicatie is gebouwd voor 40 tot 60 gebruikers, momenteel is het aantal gebruikers al het 100-voudige.

Acceptatiecriteria
De aangepaste versie van FSV voldoet aan de Archiefwetgeving en de AVG en de hiervoor beschreven wensen functioneren zoals bedoeld.

Bijlagen

Afkortingen

AFB	Adviesteam Fraude Bestendigheid
AVG	Algemene Verordening Gegevensbescherming
BI	Bestuurlijke Informatie
EHI	Expertiseteam Handhaving en Intelligence
EOS	Externe Overheids Samenwerking
MKB	Midden en Klein Bedrijf
MSNP	Minnelijke Schuldhulpverlening Natuurlijk Personen
PDB	Particulieren Dienstverlening en Bezwaar
RIEC	Regionaal Informatie en Expertise Centrum
WSNP	Wet Schuldsanering Natuurlijke Personen
IVT	InterVentieTeams
PIA	Privacy Impact Assessment
INL	Inning Lokaal

bijlage 30

Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Het Handboek Beveiliging Belastingdienst:

"U kunt op ons vertrouwen."

De Belastingdienst staat voor een betrouwbare en integere organisatie. We passen op de kroonjuwelen van belastingplichtigen, toeslaggerechtigden en partners van de Belastingdienst. Zij mogen op ons vertrouwen en als we het goed doen, vergroot hun bereidheid om aan hun verplichtingen te voldoen.

Onze betrouwbaarheid en ons imago – en daarmee het imago van de Rijksoverheid – is grotendeels gegrondvest op beveiliging, die naadloos past bij onze basiswaarden:

- *Geloofwaardigheid*. De Belastingdienst neemt zijn opdracht serieus en houdt zich aan afspraken;
- *Verantwoordelijkheid*. De Belastingdienst gaat verantwoord om met de bevoegdheden en legt hierover verantwoording af;
- *Zorgvuldigheid*. De Belastingdienst behandelt iedereen met respect en houdt rekening met verwachtingen, rechten en belangen.

Beveiliging wordt vaak gezien als noodzakelijk ongemak, terwijl we het juist goed kunnen gebruiken in onze missie: eenvoudig aanspreekbaar.

We aanvaarden bewust risico's, want alles voor honderd procent dicht timmeren willen en doen we al lang niet meer.

Wat betreft *risico's*: We gaan verder kijken dan de risico's die traditioneel in beeld zijn. In de brede context van onze maatschappelijke functie kijken we naar onze omgeving, politiek, bestuurlijk en technologisch, maar ook naar onszelf, bijvoorbeeld naar bewustwording, integriteit of digitale vaardigheid. Proportioneel, logisch en in samenhang. – Eenvoudig.
Wat betreft *bewust*: We gaan verder dan simpelweg risico's accepteren. We weten wat dat betekent voor ons en onze omgeving en onze keuzes zijn transparant, gedragen en uit te leggen. – Aanspreekbaar.

Onze basiswaarden gelden ook voor de manier waarop we beveiliging vormgeven. We kiezen voor normen die zijn gebaseerd op gezamenlijke afspraken en we houden ons hieraan, waarbij ruimte is voor verschillende invulling van maatregelen. Hierover zijn we open en samen in gesprek. We laten zien wat we doen en kunnen uitleggen waarom. De maatschappij verwacht een adequate verantwoording van ons en zo werken we ook met elkaar.

Doel en reikwijdte van het handboek

Beleidsterreinen beveiliging

Beveiliging omvat de volgende beleidsterreinen:

- *Personele veiligheid en integriteit*: de veiligheid voor medewerkers en bezoekers en de invulling van de begrippen "goed ambtenaarschap" en "goed werkgeverschap";
- *Fysieke beveiliging*: de veiligheid van gebouwen en terreinen;
- *Informatiebeveiliging*: de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie en verwerking daarvan (zowel handmatig als geautomatiseerd);
- *Bedrijfscontinuïteit*: het omgaan met risico's die de ongestoorde bedrijfsvoering van de Belastingdienst bedreigen.

CIO-agenda

Investeringsagenda

De overlap van deze terreinen met elkaar behoeft geen uitleg. Alleen in samenhang kunnen de uiteindelijke maatregelen doeltreffend en doelmatig zijn, onder de noemer van beveiliging. Dit wordt onderstreept in de CIO-agenda[1] als strategische keuze in 'continuïteit', is herkenbaar in Spoor B van de Brede agenda[2] en vervolgens in de Investeringsagenda[3].

De impact die een calamiteit heeft of kan hebben op de organisatie, bepaalt of deze op het terrein van bedrijfscontinuïteit ligt: alles wat de kritische bedrijfsfuncties kan verstoren.

Kwaliteit bedrijfsvoering

Ook bestaat samenhang met de kwaliteit van de gehele bedrijfsvoering: beveiliging is een onderdeel daarvan en zodoende ook een integraal onderdeel van de interne controle.

Doelstelling

De doelstelling van het handboek is het vastleggen van het beveiligingsbeleid en de beveiligingsnormen van de Belastingdienst. Zodoende worden de voorwaarden gecreëerd, waarmee:

- van toepassing zijnde wet- en regelgeving wordt nageleefd;
- de Belastingdienst aan zijn primaire doelstellingen kan voldoen;

MLTP

- de bereidheid van burgers en bedrijven om aan hun verplichtingen te voldoen wordt bevorderd[4];
- bedrijfsschade en persoonlijk letsel zoveel mogelijk wordt voorkomen;
- veilige (arbeids)omstandigheden worden geboden aan medewerkers en bezoekers.

Om tot een geslaagde implementatie en naleving van beveiliging binnen de Belastingdienst te komen zijn de volgende factoren van wezenlijk belang:

- één handboek beveiliging voor de gehele Belastingdienst, met de mogelijkheid en uitnodiging om als kapstok te fungeren voor aanvullingen op tactisch niveau (het *wat*) zowel als (bedrijfsonderdeel) specifieke invullingen op operationeel niveau (het *hoe*).
- een organisatieonafhankelijke opzet, met het oog op de houdbaarheid bij samenwerking met andere (overheids)partijen en in- of uitbesteding;

[1] CIO-agenda, september 2013
[2] Brede agenda Belastingdienst en bijlage, mei 2014
[3] Hoofdlijnen aanpak Belastingdienst. Activiteitenkalender, mei 2015
[4] Visie Belastingdienst, Middellangetermijnplan Belastingdienst 2014 – 2017, november 2013.

- een benadering ten aanzien van het implementeren van beveiligingsrichtlijnen die past binnen de organisatiecultuur;
- zichtbare ondersteuning en betrokkenheid van het management;
- een goed begrip van beveiligingsrisico's, risicoanalyse en risicomanagement;
- medewerkers die bekend zijn met en actief bijdragen aan realisatie van een acceptabel niveau van beveiliging;
- een evenwichtig meetsysteem, dat gebruikt wordt om de effectiviteit van het beveiligingsbeleid te beoordelen en verbeteringen aandraagt.

Doelgroepen

Het handboek is bedoeld voor het lijnmanagement en degenen die tot taak hebben organisatie, processen en facilitaire voorzieningen in te richten en medewerkers te instrueren.
Het handboek vormt de basis voor het stellen van eisen aan (externe) leveranciers van diensten. Het dient voor het stellen van betrouwbaarheidseisen aan ketenpartners, waarvan de Belastingdienst in de bedrijfsvoering afhankelijk is. Omgekeerd dient het als verantwoordingsmiddel naar ketenpartners, die voor hun bedrijfsvoering afhankelijk zijn van de Belastingdienst.
Het handboek vormt de basis voor inrichtingsadviezen door beveiligingsmedewerkers. Interne Controlemedewerkers (IC-ers) baseren hun controles mede op dit handboek.

Reikwijdte

De reikwijdte van het handboek is de gehele bedrijfsvoering van de Belastingdienst, de materiële- en immateriële eigendommen en alle personen die zich op locaties van de Belastingdienst bevinden.
Daarnaast vallen activiteiten die door de Belastingdienst zijn inbesteed of uitbesteed aan externe leveranciers, alsmede eigendommen van derden die ter beschikking staan van de Belastingdienst onder de reikwijdte van het handboek.

Indeling van het handboek

Het Handboek Beveiliging Belastingdienst bestaat uit dit algemene hoofdstuk met inleiding, doel en reikwijdte, indeling en inhoudsopgave. Het omvat verder een aantal delen, te weten:

A. **Het strategisch kader beveiliging**, met daarin de belangrijkste beleidsmatige uitgangspunten voor beveiliging. De diverse verantwoordelijkheden en hun coördinatie staan beschreven, aangevuld met definities en principes.
   De baselinebenadering, classificatie, controle en rapportage worden uitgelegd;
B. **De algemene uitvoeringsrichtlijnen**, met het tactisch kader beveiliging. De organisatie van beveiliging is weergeven met het beeld van de daarvoor benodigde rollen en functies.
   Verder wordt aandacht besteed aan risicoanalyse, het principe "pas toe

of leg uit", controle, audit en rapportage. Algemene en principiële keuzes en hogere beveiligingsniveaus worden nader belicht.

C. **De implementatierichtlijnen (normen)**[5], waarin de beveiligingsdoelstellingen langs verplichte beheersmaatregelen worden ingevuld aan de hand van implementatierichtlijnen. Het is de Belastingdienstinterpretatie van de *best practice* NEN-ISO 27002:2013;
D. **De richtlijn NEN-ISO 22313**. Dit is een aanvulling op NEN-ISO 23301 (Managementsystemen voor bedrijfscontinuïteit) en geeft praktische handvatten voor de implementatie daarvan. Er wordt uitgebreid ingegaan op de hoofdelementen van bedrijfscontinuïteit:
   - Bedrijfsimpactanalyse en risicobeoordeling;
   - Strategie voor bedrijfscontinuïteit;
   - Vaststellen en invoeren van procedures (inclusief een continuïteitsplan);
   - Oefenen en beproeven.

[5] Normen bestaan uit hierarchisch geordende beveiligingsdoelstellingen, beheersmaatregelen en implementatierichtlijnen, conform NEN-ISO 27002

Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Deel A
Strategisch Kader Beveiliging

Inhoudsopgave

Boekdata

Titel	Handboek Beveiliging Belastingdienst 2017 Deel A : Strategisch Kader Beveiliging
Versie	December 2016
Auteur	Tactisch Beveiligingsoverleg

Versie	Opmerkingen - revisies
Mei 2011	Eerste jaargang HBB Deel A
December 2012	Tweede jaargang HBB Deel A
December 2013	Derde jaargang HBB Deel A
Januari 2015	Vierde jaargang HBB Deel A
Januari 2016	Vijfde jaargang HBB Deel A
December 2016	Zesde jaargang HBB Deel A – Boekdata, titel, afkortingenlijst, actualisaties en correcties A.3.1 Omgang met extreme bedreigingen A.5 Reguliere P&C cyclus, VMR, verwijzing naar jaarplannen A.5 Dubbelingen uit deel B verwerkt

A. Strategisch kader beveiliging

A.1. Het belang en doel van beveiliging

Continuïteit van de bedrijfsprocessen

Het halen van de bedrijfsdoelstellingen van de Belastingdienst is in hoge mate afhankelijk van goed functionerende informatiesystemen. Een informatiesysteem is een geheel van gegevensverzamelingen, de daarbij behorende personen, procedures, gebouwen, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Uitval van computers, netwerken, personeel of gebouwen, het in het ongerede raken van gegevensbestanden of het onbevoegd kennis nemen dan wel manipuleren van gegevens kunnen ernstige gevolgen hebben voor de continuïteit van de bedrijfsprocessen en de persoonlijke levenssfeer (privacy) van de betrokken belastingplichtigen, toeslaggerechtigden en partners van de Belastingdienst.

Privacybescherming

In beveiliging van de verwerking van persoonsgegevens is ons uitgangspunt dat we al het noodzakelijke doen om onze publieksrechtelijke taak[6] uit te voeren, proportioneel, op de daarbij geldende grondslagen. Hierbij zoeken we voortdurend naar de minst inbreukmakende en passende manieren.

Subsidiariteit

Compliance

Indien de Belastingdienst genoemde risico's onvoldoende beheerst, kan het vertrouwen van burgers en bedrijven in de Belastingdienst worden geschaad. Dit beïnvloedt de bereidheid van belastingplichtigen om aan hun verplichtingen te voldoen nadelig.

MLTP

Het Middellangetermijnplan[7] zegt hierover: *Voor het bevorderen van compliance is cruciaal dat burgers en bedrijven vertrouwen kunnen stellen in de Belastingdienst. Dat waarmaken vraagt dat de integriteit van de dienst boven elke vorm van twijfel is verheven. Dat is het fundament onder het functioneren van de dienst. Daaraan vorm en inhoud geven is een verantwoordelijkheid van alle medewerkers van de dienst samen en vertaalt zich in de basiswaarden geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid.*

Beveiliging levert een directe bijdrage aan de compliance. Daarenboven heeft de verstoring van de continuïteit van de gegevensverwerking een directe invloed op de kasstroom naar en van de overheid en bij de Douane tevens op het (inter)nationale handelsverkeer.

Interne, externe en technologische ontwikkelingen

De Belastingdienst heeft in zijn bedrijfsvoering niet alleen met interne ontwikkelingen te maken, maar ook met maatschappelijke en technologische factoren, die van invloed zijn op beveiliging.

Context van de organisatie

De organisatie moet externe en interne onderwerpen vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om de beoogde resultaten voor informatiebeveiliging te behalen.

[6] Uitvoeringsregeling Belastingdienst 2003, januari 2013.
[7] Middellangetermijnplan Belastingdienst 2014 – 2017, november 2013

A.1.1. Interne ontwikkelingen

a. Uitgaan van vertrouwen betekent een groter belang van beveiligingsbewustzijn, houding en gedrag.

b. Bewust risico's aanvaarden vereist helderheid over wat aanvaardbaar en wat onaanvaardbaar is, samen met een duidelijke verantwoordelijkheidsverdeling.

c. Klantgerichte benadering betekent onder meer integratie van processen en daardoor extra risico's door concentratie van taken en gegevens bij één of enkele medewerkers.

d. Werk is niet exclusief gebonden aan kantoor. Wisselende omgevingen, Het Nieuwe Werken en Tijd, Plaats- en Apparaatonafhankelijk Werken vereisen dat medewerkers een goed inzicht hebben in de risico's daarvan.

e. Van-klant-tot-klantprocessen verlopen steeds vaker zonder menselijke tussenkomst, waardoor aan hoge eisen van betrouwbaarheid van informatiesystemen moet worden voldaan, ook omdat steeds grotere volumes aan gegevens in kortere tijd worden verwerkt.

A.1.2. Externe ontwikkelingen

f. Als grote uitvoeringsorganisatie spelen we een voortrekkers- en voorbeeldrol bij een aantal projecten van de e-overheid. Integratie van overheidsprocessen en samenwerking in overheidsketens vragen om organisatieonafhankelijkheid, standaardisatie van informatiebeveiliging, afstemming met ketenpartners en het afleggen van verantwoording over het naleven van beveiligingsstandaards.

g. De populariteit van sociale netwerken e.d. en de deelname van medewerkers hierin (zgn. functionele contacten met derden) vereisen een heldere definitie en begrip van "goed ambtenaarschap" en de scheiding tussen zakelijk en privé.

h. Het mede verantwoordelijk stellen van klanten en ketenpartners voor de betrouwbaarheid van brongegevens van Belastingdienstprocessen stelt hoge eisen aan betrouwbare, externe ontsluitingsmechanismen.

i. De (publieke) aandacht voor privacybescherming neemt toe en Europese ontwikkelingen nopen tot extra maatregelen voor de bescherming van persoonsgegevens.

j. Internationale samenwerking en verdragen tot gegevensuitwisseling vereisen een vastgesteld en controleerbaar niveau van beveiliging.

A.1.3. Technologische ontwikkelingen

k. Het gebruik van de veelzijdige en voortdurend veranderende (externe) communicatiemiddelen vraagt om continue evaluatie van risico's en de manier waarop deze middelen worden gebruikt. Hieronder valt ook de trend van consumerization: nieuwe technologieën en toepassingen breken eerst door in de consumentenmarkt en van daaruit, onder druk

van de gebruikers, in organisaties. Bovendien zijn steeds meer apparaten constant online - verbonden met internet - waardoor er voortdurend dreiging bestaat. Consumerization omvat niet alleen apparatuur maar ook onlinediensten en de snelle ontwikkeling van *apps*.

l. Standaardisatie van de gegevensuitwisseling betekent een verruiming van de koppelingsmogelijkheden waardoor de risico's van onbevoegde veranderingen en kennisneming bij gegevensuitwisseling toenemen.

A.2. Beveiligingsprincipes

De principes van de Belastingdienst bestaan uit bedrijfs-, sturings-, inrichtings- en beveiligingsprincipes. De laatste twee groepen bevatten de uitgangspunten voor beveiliging:

De Belastingdienst maakt bewuste keuzes op basis van aanvaardbaar risico (inrichtingsprincipe).
Op basis van risicobeheersing maken we gemotiveerde keuzes voor beveiliging met het oog op bedrijfscontinuïteit, een veilige werkomgeving en een betrouwbare informatievoorziening.

a. Beveiliging zit in het ontwerp van processen, producten, diensten en gebouwen.
Vanaf de start van het ontwerp van processen, producten, diensten en gebouwen nemen we beveiliging mee en is daarmee een integraal onderdeel van de informatievoorziening. In principe wordt niets in gebruik genomen zonder dat er aandacht aan beveiliging is besteed.

b. Beveiliging gaat uit van een basisniveau met beperkte aanvullingen.
Beveiliging definiëren we op een doelmatig generiek niveau, de baseline. Waar verhoogde risico's bestaan treffen we aanvullende maatregelen, zoals bij vips of bijzondere opsporingsinformatie.
Op basis van aanvaardbaar risico kiezen we voor het geschikte niveau. Dit maakt beveiliging instelbaar.

c. Beveiliging biedt toegang tot de benodigde bedrijfsmiddelen.
We autoriseren medewerkers tot het raadplegen en verwerken van die gegevens, het binnentreden van die ruimten en het gebruik van die middelen, die zij voor hun werk nodig kunnen hebben: need-to-do.

d. Beveiliging werkt vanuit het eigen beveiligingsbewustzijn.
Het uitgangspunt is het vertrouwen in de eigen medewerkers, die bedrijfsmiddelen gebruiken waarvoor ze bedoeld zijn. Ze raadplegen alleen die gegevens en gebruiken alleen die ruimten of middelen die ze nodig hebben: need-to-know.

e. Beveiliging houden we simpel.
Duidelijke en eenvoudige opzet van beveiliging bevordert doelmatigheid, doeltreffendheid, acceptatie en beheersbaarheid.

f. Beveiliging ondersteunt het werk.
Beveiliging draagt bij aan een onverstoorde bedrijfsvoering en werpt geen onnodige belemmeringen op.

A.3. Risicobeheersing

Uitgangspunten risicomanagement

Bedrijfsvoering adresseert risicomanagement en streeft er naar dat[8]:

- het management zich bewust is van de impact van risico's op het realiseren van de bedrijfsdoelstellingen;
- risico's continu, expliciet en systematisch geïdentificeerd en geanalyseerd worden;
- risico's voortdurend gewogen worden;
- maatregelen toegesneden zijn op het handhaven van de acceptabel geachte risiconiveaus.

Doelstellingen hierarchie

Risico's zijn altijd gekoppeld aan doelen. Een risico wordt immers gedefinieerd als de mogelijke oorzaak van het niet halen van doelen. Een belangrijk element voor adequaat risicomanagement is dan ook een heldere doelstellingenhiërarchie, waarmee duidelijk wordt welke doelstellingen moeten worden gehaald.

Risicomanagement omvat volgens het Risicomodel Belastingdienst een veelheid van risico's, zoals:

- omgevingsrisico's zoals uit de politiek, wetgeving, maatschappelijke ontwikkelingen, imago, behoeften van burgers en bedrijven;
- procesrisico's zoals in logistiek en operatie, financiën, integriteit, ICT;
- informatie- en sturingsrisico's vanuit strategie, organisatie en besturing, verantwoording en rapportage en empowerment.

Positie van beveiliging

In het HBB staan beleid, beheersmaatregelen en implementatierichtlijnen uitgewerkt. Deze zijn een onderdeel van de verzameling maatregelen om bovenstaande bedrijfsrisico's te beheersen. Ook hieruit blijkt dat beveiliging een integraal onderdeel is van de gehele bedrijfsvoering, zoals eerder gesteld.

A.3.1. Bedreigingen voor beveiliging

Risico's betreffen de kans dat bedreigingen zich voordoen, gerelateerd aan de schade die het risico kan veroorzaken en de blootstelling aan het risico.

Specifieke bedreigingen

Traditioneel houden inbreuken op de beveiliging van gegevens en processen in dat niet-geautoriseerde personen processen en functies kunnen activeren of toevoegen, waardoor ze gegevens kunnen raadplegen, muteren, toevoegen of vernietigen. Ook kunnen infrastructurele voorzieningen buiten gebruik worden gesteld door personen, technisch falen en door "natuurlijke" bedreigingen zoals storm en blikseminslag.

Bedreigingen worden daarbij veroorzaakt door:

- personen (derden en eigen medewerkers, al dan niet opzettelijk), die verantwoordelijk zijn voor fouten, datalekken, diefstal, fraude, staking, sabotage, omkoping, afluisteren, verbale of fysieke agressie;
- technisch falen, veroorzaakt door bijvoorbeeld brand, water- en weersoverlast, virussen, apparatuur- en softwarestoringen.

[8] *Beleidsplan Risicomanagement* v2 1, november 2008

Actuele bedreigingen

Op basis van het *Cybersecuritybeeld Nederland*[9] hebben we aanvullend verhoogde aandacht voor digitale spionage, digitale identiteitsfraude, verstoring van online dienstverlening en datalekken zoals (al dan niet bewuste) publicatie van vertrouwelijke informatie.
Ook criminele organisaties, beroepscriminelen en buitenlandse actoren/inlichtingendiensten zijn relevant voor de Belastingdienst. Met name de groepen die zich structureel bezighouden met *hightechcrime* op basis van innovatieve methoden vormen een steeds grotere bedreiging.

Spionage

Cruciale belangen

Naar aanleiding van de *Kwetsbaarheidsanalyse Spionage (KWAS)* van de AIVD[10] en de kabinetsreactie[11] hierop is de *Handleiding KWAS*[12] uitgebracht. Het is van belang om op basis van deze handleiding in kaart te hebben gebracht welke *cruciale belangen* worden onderkend en of deze afdoende beschermd zijn. Onder cruciaal belang wordt informatie van het eigen departement verstaan waarvan:

- kennisname door anderen dan direct belanghebbenden de veiligheid of andere gewichtige belangen van de staat of haar bondgenoten kan worden aangetast en/of
- verondersteld kan worden dat buitenlandse inlichtingendiensten er belang bij hebben deze te bezitten.

Terreur

De Belastingdienst houdt in het (basis)beveiligingsbeleid geen rekening met extreme bedreigingen zoals gewapende conflicten, daden van terreur, atoomkernreacties en aardbevingen. De omgang met extreme bedreigingen valt in het gebied van crisismanagement en bedrijfscontinuïteit. De processen van de Belastingdienst worden niet gerekend tot de vitale infrastructuur van Nederland[13].

A.3.2. Beveiligingsbewustzijn

Houding en gedrag

Beveiliging kan zeker niet alleen rusten op procedures en techniek. Het is vooral ook een kwestie van mentaliteit van medewerkers, die techniek of procedures bewust of onbewust zouden kunnen omzeilen. Het gedrag van medewerkers is sterk medebepalend voor de beheersing van de risico's.

MLTP

Het MLTP stelt: *Iedere medewerker neemt zijn verantwoordelijkheid, en krijgt kansen en professionele ruimte.*
Het is de verantwoordelijkheid van de medewerker om zorgvuldig met beveiliging om te gaan.

Bevorderen beveiligings-bewustzijn

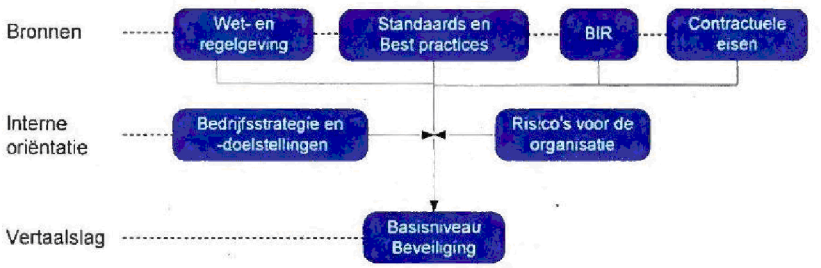
Aanvullend kiest de Belastingdienst voor een structurele en periodieke voorlichting aan zijn medewerkers. Het lijnmanagement is verantwoordelijk voor het stelselmatig bevorderen van het beveiligingsbewustzijn.

[9] VenJ/NCSC, Cybersecuritybeeld Nederland CSBN-3, november 2013
[10] TK 2010–2011, 30 821, nr 11
[11] TK 2010–2011, 30 821, nr 13
[12] BZK/AIVD en VenJ/DG Veiligheid, januari 2011
[13] Rapport *Bescherming vitale infrastructuur*, paragraaf 2.7, BZK/NAVI, september 2005.

A.3.3. Basisniveau beveiliging: risicoanalyse

Basisniveau Beveiliging

Voor zover beveiligingsrisico's algemeen van aard zijn, d.w.z. niet specifiek zijn voor de Belastingdienst, spelen de standaarden en *best practices* die mede als referentie gelden voor dit handboek, hierop voldoende in. Uit de combinatie van de bestaande kaders wordt het basisniveau beveiliging afgeleid.



Figuur 1: Afleiden basisniveau beveiliging

Wet- en regelgeving

De belangrijkste wet- en regelgeving is: de Ambtenarenwet (Aw) en het Algemeen rijksambtenarenreglement (ARAR), de PUB (Personele Uitvoeringsbepalingen Belastingdienst), de Algemene wet bestuursrecht (Awb), de Wet computercriminaliteit (Wcc), de Wet bescherming persoonsgegevens (Wbp[14]), de Wet elektronische handtekeningen (Weh), het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR), het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013), het Besluit beveiligingsvoorschrift rijksdienst 2013, de Archiefwet en de Arbowet.
Voor de FIOD is voorts de Wet politiegegevens (Wpg) relevant.

Standaarden en *best practices*

Als standaarden en *best practices* worden gehanteerd: NEN-ISO 27001 Management Systemen voor Informatiebeveiliging en NEN-ISO 27002:2013, die zijn voorgeschreven onder het regime "pas toe of leg uit" door het Forum Standaardisatie voor de Nederlandse overheid. In dat kader zijn eveneens van toepassing de afgeleide principes voor Sturing en verantwoordelijkheid, respectievelijk Betrouwbaarheid van de Nederlandse Overheids Referentie Architectuur (NORA) versie 3.0 en het dossier Informatiebeveiliging. Voor Bedrijfscontinuïteit is de NEN-ISO 22301 en 22313 als meest gebruikte standaard van toepassing.

NEN-ISO 27002

NEN-ISO 22301

De richtlijnen en normen van HBB Deel C omvat de NEN-ISO 27002:2013. Een cross-reference[15] in twee richtingen maakt een vergelijking van de normen uit beide kaders mogelijk. HBB Deel D omvat de NEN-ISO 22313.

BIR

De Baseline Informatiebeveiliging Rijksdienst (BIR) is het normenkader voor informatiebeveiliging dat door het ICCIO is vastgesteld voor de Rijksdienst. We voldoen hieraan op basis van HBB Deel C volgens *comply or explain* zoals we zelf bij implementatie van het HBB hanteren.

.....

[14] Inclusief de recente wijziging in het kader van de *meldplicht datalekken*.
[15] De cross-reference staat op Belastingnet/CSOnet.

Contractuele eisen hebben betrekking op afspraken gemaakt met ketenpartners. Als deze de eigen Belastingdienstuitgangspunten overstijgen, worden ze in het handboek aangevuld.

A.3.4. Basisniveau beveiliging: classificatie

Hoog basisniveau van beveiliging

De Belastingdienst hanteert een niveau van beveiliging dat gericht is op de beveiliging van massale verwerking van persoons- en financieel-economische gegevens. Dit niveau van beveiliging is gemiddeld genomen voor alle informatiesystemen tevens het basisniveau omdat voor wat betreft beveiliging de processen en gegevens voor een groot deel gelijkwaardig zijn. Een voordeel hiervan is ook dat het basisniveau beveiliging met generieke normen kan worden ingevuld. Dit vereenvoudigt het beheer en beperkt de kosten. Deze normen liggen op het niveau van Departementaal Vertrouwelijk volgens het VIRBI. De uitwerking en evaluatie van het niveau wordt mede gebaseerd op de uitwerking in de BIR.

Bijzondere informatie

Bij de Belastingdienst wordt in de regel[16] geen bijzondere informatie volgens VIRBI gegenereerd. Voor zover de Belastingdienst bijzondere informatie onder zich heeft, bestaat deze uit als zodanig geclassificeerde bijzondere informatie, welke is aangeleverd door andere handhavingspartners. Informatie die de Belastingdienst aan bijzondere informatie van derden toevoegt, valt daarmee onder die rubricering. In principe wordt geen bijzondere informatie in digitale vorm door de Belastingdienst ontvangen of verzonden.

Vertrouwensfuncties

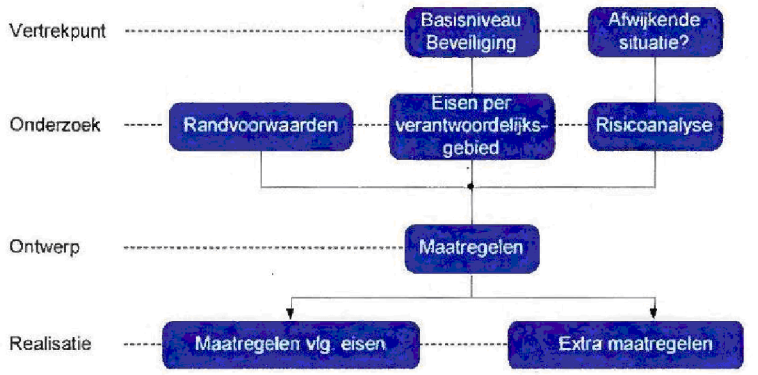
In de Belastingdienst zijn vertrouwensfuncties aan te wijzen. Het gaat om functies waarin de functionaris de nationale veiligheid kan schaden[17] en waarvoor een veiligheidsonderzoek noodzakelijk is. Daarnaast worden veiligheidsonderzoeken ingesteld indien de samenwerking met externe partners dit vereist.

[16] Uitzonderingen bestaan bijvoorbeeld bij gegevensverwerking door de FIOD
[17] Conform de *Leidraad aanwijzing vertrouwensfuncties*, september 2014, BZK/AIVD

A.3.5. Basisniveau beveiliging: het treffen van maatregelen

Cyclisch onderhoud

Op basis van de bedrijfsdoelstellingen en risico's wordt op cyclische wijze onderhoud gepleegd aan de bestaande handboeken, die invulling geven aan het begrip *basisniveau beveiliging*. Ook komen risico's aan de orde bij het treffen van maatregelen per verantwoordelijkheidsgebied.



Figuur 2: Onderhoud maatregelen

Toelichting bij de figuur:

- Voor het merendeel van de verantwoordelijkheidsgebieden worden de maatregelen getroffen volgens het basisniveau. Daarbij is het van belang om vooral bij vernieuwingen en onderhoud van verantwoordelijkheidsgebieden van beveiliging vast te stellen of er sprake is van afwijkende situaties, die risico's met zich brengen die onvoldoende in het basisniveau zijn inbegrepen. Afwijkende situaties bij informatiesystemen kunnen onder meer betrekking hebben op hogere beschikbaarheidseisen, anders dan standaard gebruik van bestaande technologie, toepassing van nieuwe technologie, gegevens met een bijzonder belang en conversieproblematiek.
- Er zijn meer factoren op grond waarvan er in specifieke situaties afgeweken kan worden van de implementatierichtlijnen: te hoge kosten, onvoldoende haalbaarheid, de mate van effectiviteit in de specifieke situatie, de ouderdom van het gebouw of informatiesysteem etc. Die factoren worden hier samengevat onder het begrip "randvoorwaarden".
- Verantwoordelijkheidsgebieden corresponderen met de onderdelen van dit handboek en de indeling van de normen.

A.4. Organisatie van beveiliging

Verantwoordelijkheids-verdeling

Beveiliging is als onderdeel van integraal management en bedrijfsvoering een verantwoordelijkheid van het lijnmanagement op de diverse niveaus in de organisatie.
Op het hoogste niveau binnen de Belastingdienst geldt de volgende verdeling van beveiligingsverantwoordelijkheden:

- de eindverantwoordelijkheid ligt bij de Chief Security Officer (CSO), alsook de verantwoordelijkheid voor bedrijfscontinuïteit;
- de verantwoordelijkheid voor personele veiligheid en integriteit bij de Chief Personnel Officer (CHRO), het concernpersoneelsbeleid;

- de verantwoordelijkheid voor informatiebeveiliging bij de Chief Information Officer (CIO);
- de verantwoordelijkheid voor fysieke beveiliging bij het verantwoordelijke MT-lid van B/CFD.

A.4.1. Strategische beveiliging in het MT-Belastingdienst

MT-Belastingdienst

Beveiliging wordt structureel geagendeerd in het MT-Belastingdienst. De structuur van het Strategisch Beveiligingsoverleg (SBO) is overgegaan in het MT BD *special* of *open space*. Vooroverleg vindt plaats tussen de CSO en de verantwoordelijken voor de drie aspectgebieden.

Het MT-Belastingdienst bepaalt het beleid en bespreekt de (jaarlijkse) rapportages van de bedrijfsonderdelen. De CSO stemt af met de beveiligingsambtenaar van het Ministerie van Financiën en communiceert in de lijn via het overleg van de Chief Financial Officers (CFO's).

Jaarlijks worden door de CSO met de ADR afspraken gemaakt over de thema's waarover gerapporteerd of waarop gecertificeerd dient te worden en waarop een (eventuele) externe audit zal worden uitgevoerd om extra zekerheid te verkrijgen over de implementatie van beveiligingsrichtlijnen.

A.4.2. Tactisch Beveiligingsoverleg (TBO)

Doel TBO

Het TBO is een adviesorgaan voor het MT-Belastingdienst. Het is beleidsvoorbereidend en evaluerend en kent een lijnsturing. Het geeft gevraagd en ongevraagd advies aan de CSO, CIO, CHRO of de CFO van een bedrijfsonderdeel. Het TBO dient voor de afstemming tussen het strategisch niveau en de bedrijfsonderdelen.
De deelnemers zijn vertegenwoordigers van alle bedrijfsonderdelen.

A.4.3. Clusters en kennisgroepen

Doel clusters

Voor de verschillende beleidsgebieden van beveiliging zijn clusters of kennisgroepen geformeerd, waarin onder meer beveiligingsadviseurs en beveiligingsmedewerkers van bedrijfsonderdelen de onderwerpen van bespreking in het TBO voorbereiden. Ook hier zijn de deelnemers vertegenwoordigers van de bedrijfsonderdelen.

Deze groepen zijn:

- Cluster Business Continuity Management;
- Cluster Informatiebeveiliging;
- Cluster Fysieke Beveiliging
- Cluster Personele Veiligheid en Integriteit;
- Kennisgroep Integriteit.

A.4.4. Beveiligingsbeheersingscyclus

Het VIR geeft de beveiligingsbeheersingscyclus op deze wijze weer:

Proces voor risicobeheersing

Figuur 3: Beheersingscyclus

De betrouwbaarheidseisen (hier verder beveiligingseisen genoemd) komen tot uitdrukking in de doelstellingen en implementatierichtlijnen zoals deze in dit handboek zijn uitgewerkt.
De feitelijke maatregelen worden op basis van de normen in dit handboek ontworpen. Voor geautomatiseerde systemen bijvoorbeeld door informatiemanagement en procesinrichting. De normen vormen tevens onderdeel van de in- en externe controle. Leemten, die bij controles zijn vastgesteld, geven aanleiding tot het aanpassen van de feitelijke maatregelen. Incidentrapportage, uitzonderingsrapportage, uitkomsten van de controles en veranderde in- en externe omgevingsfactoren worden als input gebruikt voor evaluatie en bijstelling van de beveiligingseisen.
Over de check- en actfase wordt teruggerapporteerd aan de Chief Security Officer. De beheersingscyclus speelt zich feitelijk af op zowel het strategische, tactische als operationele niveau van de Belastingdienst.

De verantwoordelijkheden voor het lijnmanagement op het hoogste niveau zijn als volgt:

Plan: Beveiligingseisen

- visievorming op de betekenis van beveiliging door voortdurende beeldvorming over risico's en oplossingsrichtingen voor maatregelen passend bij het Belastingdienstbeleid;
- vaststellen doelen voor beveiliging en beleid om die doelen te bereiken;
- toewijzen van de beveiligingsverantwoordelijkheden voor interne en externe ketens van informatiesystemen aan lijnmanagers;
- toewijzen verantwoordelijkheden voor de naleving van de privacywetgeving.

Do: Treffen maatregelen

- goedkeuren uitvoeringsrichtlijnen;
- bijdragen aan voorlichtings-, bewustwordings- en opleidingsprogramma's voor beveiliging;
- besluitvorming over belangrijke afwijkingen van normen en accepteren restrisico's.

Check: Controle

- het voeren van de centrale regie bij geven van periodieke en incidentele opdrachten tot het verrichten van interne onderzoeken en (externe) audits;
- beoordelen van interne en externe (audit)rapportages over beveiliging en toezien op de naleving van afspraken over oplossing van leemten.

Act. Evaluatie en aanpassen

- beoordelen ontwikkelingen in de maatschappij en de relevante omgeving voor de Belastingdienst;
- beoordelen van incidentrapportage;
- evalueren resultaten checkfase;
- geven van opdrachten tot bijstelling van visie en beleid en aanpassing van uitvoeringsrichtlijnen op basis van evaluaties.

A.5. Rapportage, planning- en controlcyclus

Prestatie-indicatoren meten via controle

De kwaliteit van de bedrijfsvoering wordt geborgd door te werken volgens de Planning en Control (P&C) cyclus. Dit is de jaarlijkse terugkerende beleids-, begrotings- en verantwoordingscyclus waarbinnen alle relevante bedrijfsvoeringaspecten in samenhang een plaats hebben. De interne sturing maakt daarbij gebruik van SMART geformuleerde prestatie-indicatoren.

Jaarplannen

Om tot een evenwichtig, samenhangend en afdoend stelsel van beveiligingsmaatregelen te komen worden de beveiligingsaspecten, voorzien van prestatie-indicatoren, opgenomen in de jaarplannen van de bedrijfsonderdelen en in de P&C cyclus. De prestatie-indicatoren voor beveiliging zijn de beheersmaatregelen uit dit handboek. Het meten geschiedt via in- en externe controle.

VMR

De bedrijfsonderdelen zijn verplicht ten behoeve van de viermaandsrapportages verantwoording af te leggen over de beveiligingsdoelstellingen uit het HBB, in het bijzonder over de beveiligingsdoelstellingen die jaarlijks door het MT BD worden vastgesteld.

Rapportage aan CSO

Aan de CSO wordt voor 15 maart gerapporteerd over het voorgaande jaar. Daarnaast wordt gerapporteerd op basis van ad hoc vragen bijvoorbeeld uit het MT-Belastingdienst, de Rijksinspecties of de Algemene Rekenkamer. De rapportages worden in het TBO besproken en vormen input voor het beheersverslag Belastingdienst.

Wanneer een bedrijfsonderdeel met inachtneming van *comply or explain* niet voldoet aan het HBB meldt het desbetreffende management dit aan de CSO. Als het gevolg hiervan is dat niet wordt voldaan aan wet- en regelgeving meldt de CSO dit aan het Ministerie van BZK.

ICP

De actuele versie van het intern controleprogramma (ICP) staat gepubliceerd op Belastingnet/CSO-net. Het ICP richt zich als handreiking primair op de algemene, centraal vastgestelde beveiligingsdoelstellingen. Indien er per bedrijfsonderdeel op basis van een eigen risicobeoordeling wordt afgeweken van de centrale afspraken over de uitvoering van het ICP, wordt dit in de rapportage toegelicht.

In control statement

Er wordt onder meer ten behoeve van ketenpartners, burgers en bedrijven verantwoording afgelegd in een *in control statement* in het jaarverslag en de uitzonderingsrapportage. Hierbij verklaart het management van de Belastingdienst dat de interne risicobeheersings- en controlesystemen adequaat en effectief zijn.

A.6. Kosten

Kosten als onderdeel van investeringsbeslissingen

Inherent aan het uitgangspunt dat beveiliging een integrale management-verantwoordelijkheid is, komen de kosten van beveiliging ten laste van de budgetten van de verantwoordelijke lijnmanagers. De financiering geschiedt daarmee via de reguliere budgetcyclus van de Belastingdienst. Kosten van fysieke beveiliging zijn een apart onderdeel van de Huisvestingsnota.

Gebruikte afkortingen

ADR	Auditdienst Rijk
AIVD	Algemene Inlichtingen- en Veiligheidsdienst (BZK)
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CFD	Centrum voor Facilitaire Dienstverlening
CFO	Chief Financial Officer
CHRO	Chief Human Resource Officer
CIO	Chief Information Officer
CSO	Chief Security Officer
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HBB	Handboek Beveiliging Belastingdienst
ICCIO	Interdepartementale Commissie Chief Information Officers
MLTP	Middellangetermijnplan Belastingdienst 2014 - 2017
MT	Managementteam
NAVI	Nationaal Adviescentrum Vitale Infrastructuur
NCSC	Nationaal Cyber Security Centrum
P&C	Planning en Control
PUB	Personele Uitvoeringsbepalingen Belastingdienst
SBO	Strategisch beveiligingsoverleg
SMART	Specifiek, meetbaar, acceptabel, realistisch en tijdgebonden
TBO	Tactisch beveiligingsoverleg
VenJ	Ministerie van Veiligheid en Justitie

bylage 31

Ministerie van Financiën

Handboek Beveiliging Belastingdienst

2017

Deel B

Algemene Uitvoeringsrichtlijnen

Inhoudsopgave

Boekdata

Titel	Handboek Beveiliging Belastingdienst 2017 Deel B : Algemene Uitvoeringsrichtlijnen
Versie	December 2017
Auteur	Tactisch Beveiligingsoverleg

Versie	Opmerkingen - revisies
Mei 2011	Eerste jaargang HBB Deel B
December 2012	Tweede jaargang HBB Deel B
December 2013	Derde jaargang HBB Deel B
Januari 2015	Vierde jaargang HBB Deel B
Februari 2016	Vijfde jaargang HBB Deel B
December 2016	Zesde jaargang HBB Deel B – Boekdata, titel, afkortingenlijst en correcties – Inhoudelijke aanpassingen en actualisaties B. Redactie en technisch beheer verwijderd B.1.1.3 Ambtenaren Belastingdienst B.1.2 BCM als lijnverantwoordelijkheid B.1.2 BCMM als implementatiemodel B.1.2.2 Crisiscommunicatie B.1.2.3 Continuïteitsstrategie B.1.2.5 Fysieke uitwijk in eigen gebouwen B.1.3.2.4 Gebruik van live/productiegegevens B.1.3.2.5 Beveiligingsfuncties, herleidbaarheid B.1.4 Encryptie bij transport en opslag B.1.4 Bedrijfsgegevens uitsluitend op bedrijfsmiddelen B.1.4 Gevonden gegevensdragers B.1.7 Geen hyperlinks in e-mail B.1.7 Black- en whitelisting bij internettoegang B.1.2.4 Inzet BHV-organisatie B.1.2.5 Fysieke uitwijk Belastingdienstgebouwen B.2.2 Dreigingsprofiel opgenomen in A.3.1 B.5 Rapportage en intern controleprogramma opgenomen in A.5

B. Algemene uitvoeringsrichtlijnen

Leeswijzer	In deel B van het Handboek Beveiliging Belastingdienst worden uitvoeringsrichtlijnen voor beveiliging uitgewerkt op basis van deel A, het strategisch kader. Het betreft tactische beleidsuitgangspunten en beveiligingsrichtlijnen, die voor de hele organisatie van de Belastingdienst gelden. De organisatie van beveiliging wordt op basis van het strategisch kader uitgewerkt. Daarnaast wordt toelichting gegeven op de structuur en het gebruik van de implementatierichtlijnen.
Beheer HBB	Het inhoudelijk beheer van het HBB wordt gevoerd door de clusters/kennisgroepen en goedgekeurd door het Tactisch Beveiligingsoverleg. Hieronder valt ook de verwerking van eventuele wijzigingen in de gebruikte standaarden en *best practices*.
Updatefrequentie	Minimaal één maal per kalenderjaar worden wijzigingen in het HBB formeel doorgevoerd. Dit betreft bijvoorbeeld updates, verwerking van wijzigingen in de standaarden of rijksoverheidskaders, input uit implementatieresultaten en voortschrijdend inzicht.
Brondocument	In het Tactisch Beveiligingsoverleg (TBO) wordt de nieuwe versie goedgekeurd en ter vaststelling aan het MT Belastingdienst aangeboden. De meest actuele en leidende versie van het HBB is de digitale (web)versie op Belastingnet.

B.1. Tactisch kader beveiliging

Het strategisch kader beveiliging geeft de belangrijkste beleidsmatige uitgangspunten voor beveiliging. Ze zijn ingegeven door de beveiligingsprincipes en liggen in het verlengde van de kwaliteit van de gehele bedrijfsvoering van de Belastingdienst. Ze worden benaderd vanuit de aspecten *personele veiligheid en integriteit*, *fysieke beveiliging*, *informatiebeveiliging* en *bedrijfscontinuïteit*.

Vier aspecten

Privacybescherming, de beveiliging van de verwerking van persoonsgegevens, is een integraal onderdeel van de beveiliging.

Privacy

Het tactisch kader beveiliging geeft de algemene uitvoeringsrichtlijnen en beleidsuitgangspunten voor de inrichting van beveiliging, waarbij rekening wordt gehouden met de gescheiden verantwoordelijkheid ten opzichte van de uitvoering: ze hebben namelijk voor het merendeel betrekking op verschillende aspecten tegelijk, waarbij de samenhang geborgd moet zijn.

Positie tactisch kader beveiliging

Zodoende kan de verantwoordelijkheid voor een enkele maatregel uit het samenhangende stelsel op hoger lijnniveau worden gepositioneerd.

De beleidsuitgangspunten en uitvoeringsrichtlijnen in dit tactisch kader zijn in eerste instantie geordend naar de beleidsthema's die volgen uit de NEN-ISO 27002:2013. Het volgen van de thema's uit deze standaard zorgt voor een universele, organisatieonafhankelijke en uitwisselbare opzet.

Daar waar het van toepassing is, wordt de samenhang over de aspecten heen aangegeven.

B.1.1. Beleid op het classificeren van informatie

De Belastingdienst hanteert een niveau van beveiliging dat gericht is op de beveiliging van massale verwerking van persoons- en financieel-economische gegevens, overeenkomend met de eertijds door het College Bescherming Persoonsgegevens[1] beschreven risicoklasse II, verhoogd risico. De indeling in risicoklassen is losgelaten bij de publicatie van nieuwe beleidsregels[2] (richtsnoer) voor de beveiliging van persoonsgegevens.

B.1.1.1. Basis beveiligingsniveau

Het hiervoor genoemde niveau van beveiliging is gemiddeld genomen voor alle informatiesystemen tevens het basisniveau omdat voor wat betreft beveiliging de processen en gegevens voor een groot deel gelijkwaardig zijn. Een voordeel hiervan is dat het basisniveau beveiliging met generieke normen kan worden ingevuld. Dit vereenvoudigt het beheer en beperkt de kosten.

Binnen het basis beveiligingsniveau is op onderdelen wel sprake van differentiatie in beveiligingsniveau, zoals bij de fysieke, logische en netwerkzonering. Bij netwerkzonering hanteren we modellen die in de normering zijn uitgewerkt. Zie daarvoor ook de HBB bijlage IB-patronen op CSO-net.

Daarnaast is ook sprake van differentiatie bij papieren en elektronische gegevens met een verhoogd risico, bijvoorbeeld bij gegevens van bedrijven

[1] Per januari 2016 de Autoriteit Persoonsgegevens
[2] https //autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens pdf

waarvan de Belastingdienst koersgevoelige informatie bezit. In die gevallen worden per bedrijfsonderdeel onder verantwoordelijkheid van het desbetreffende management aanvullende maatregelen getroffen met betrekking tot procedures en personeel.

B.1.1.2. Bijzondere informatie

VIRBI

De informatie binnen de Belastingdienst wordt overeenkomstig het niveau *departementaal vertrouwelijk* volgens het VIRBI[3] beschermd. Er wordt in de regel geen bijzondere informatie gegenereerd op het niveau van *staatsgeheim-confidentieel* of hoger, met uitzondering van bepaalde gegevens van de FIOD. Met betrekking tot die gegevens worden op basis van ketenafspraken met andere inspectiediensten afzonderlijke maatregelen getroffen ter voldoening aan het VIRBI. Voor de bepaling van de rubricering gebruiken we de richtlijnen van de Rijksoverheid[4].

Voor zover de Belastingdienst verder bijzondere informatie op het niveau van staatsgeheim-confidentieel of hoger onder zich heeft, bestaat deze uit als zodanig geclassificeerde bijzondere informatie, welke is aangeleverd door andere (handhavings)partners.

Informatie die de Belastingdienst aan bijzondere informatie van derden toevoegt, valt daarmee onder die rubricering. In principe wordt geen bijzondere informatie op het niveau van staatsgeheim-confidentieel of hoger in digitale vorm door de Belastingdienst ontvangen of verzonden, behalve in bepaalde gevallen bij de FIOD. Er geldt een aparte classificatie voor *very important persons* (vips). De beveiligingsmaatregelen behorend bij die gegevensklasse worden op een algemeen hoger niveau procedureel uitgewerkt.

B.1.1.3. Vips

De posten voor *very important persons* worden gebruikt om de toegang tot fiscale gegevens van bepaalde personen aan een beperkt aantal daartoe aangewezen functionarissen toe te wijzen.

Vips

Vips zijn personen met specifieke te beschermen functies (Koninklijk Huis, bewindspersonen etc.). DGBel/Cluster Fiscaliteit bewaakt de mutaties hiervan en geeft deze door aan B/CA waar de personen vervolgens worden gemerkt in de systemen.

Ambtenaren Belastingdienst

Naast de gegevens van Vips worden uit het oogpunt van zorgvuldigheid ook de gegevens van de ambtenaren van de Belastingdienst op eenzelfde wijze afgeschermd.

Afscherming

In principe biedt het basisstelsel van maatregelen afdoende afscherming voor deze categorie. Extra afscherming kan worden toegepast mits dit proportioneel is. Voor de Belastingdienstmedewerkers dient de extra aandacht voor integriteit te blijven bij de afhandeling van de aangiftes.

Bij applicatieontwikkeling dient er rekening te worden gehouden met de mogelijkheid tot het afschermen van personen.

[3] Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
[4] Handleiding Rubricering v1.7, IBR, juni 2015

B.1.1.4. Vertrouwensfuncties

Besluit vakminister

De Wet veiligheidsonderzoeken bepaalt dat functies die de mogelijkheid bieden de nationale veiligheid te schaden, door de verantwoordelijke minister worden aangewezen als vertrouwensfuncties. Deze vakminister is verantwoordelijk voor het juist doorlopen van het afwegingsproces en wijst met een besluit[5] vertrouwensfuncties aan.

Een vertrouwensfunctie wordt als zodanig aangewezen als er sprake is van tenminste één van de volgende drie criteria.

- De functie geeft structureel toegang tot kwetsbare en/of staatsgeheime informatie en/of kernbelangen die bij compromittering schade aan de nationale veiligheid veroorzaken (informatie);
- De functie geeft directe, ongecontroleerde toegang tot mogelijke doelwitten of middelen die een aanslag of spionage faciliteren, waarbij in alle gevallen schade aan de nationale veiligheid ontstaat (toegang);
- De functie is een sleutelpositie in een organisatie die de democratische rechtsorde bewaakt en is daarmee een nationale voorbeeldfunctie (boegbeeld).

Leidraad AIVD

Voor de aanwijzing van vertrouwensfuncties wordt de leidraad[6] van de AIVD gehanteerd. Het management van een bedrijfsonderdeel geeft binnen de kaders van de leidraad aan of en zo ja welke functies er binnen het eigen bedrijfsonderdeel als vertrouwensfuncties dienen te worden aangewezen en van welk niveau het veiligheidsonderzoek dient te zijn en houdt dit actueel.

B.1.1.5. Kritische en risicovolle functies

Kritische en risicovolle functies zijn functies die invloed kunnen hebben op de bedrijfscontinuïteit of de integriteit van de Belastingdienst. We definiëren deze als volgt:

Bedrijfsproces

- Kritische functies zijn functies waarbij de voortgang van een kritisch bedrijfsproces ernstig in gevaar komt bij uitval van medewerkers;

Integriteitsinbreuk

- Risicovolle (of kwetsbare) functies zijn functies die risico's op integriteitsinbreuken met zich mee brengen, door bijvoorbeeld het werken met gevoelige informatie, het kunnen beschikken over geld en de omgang met zakelijke relaties.

Elk bedrijfsonderdeel van de Belastingdienst kan geconfronteerd worden met integriteitsinbreuken en/of stagnatie van de bedrijfscontinuïteit. Deze kunnen voortkomen uit het in onvoldoende mate nemen van maatregelen tegen de risico's die zich voor kunnen doen bij het uitoefenen van kritische, risicovolle en/of vertrouwensfuncties.

De kritische en risicovolle functies, de risico's daarvan en de maatregelen die zijn getroffen worden daarom door de leidinggevende in kaart gebracht, geregistreerd en door het management vastgesteld.

Het vaststellen van de kwetsbare functies door het management helpt de organisatie zicht te houden op de risico's die worden gelopen en vergroot het bewustzijn en het draagvlak voor de te nemen maatregelen.

[5] Conform de Algemene wet bestuursrecht
[6] *Leidraad aanwijzing vertrouwensfuncties*, september 2014, BZK/AIVD

B.1.2. Beleid op bedrijfscontinuïteit

Lijnverantwoording

Business Continuity Management (BCM) is een samenhangend geheel aan activiteiten dat er op is gericht de continuïteit van de organisatie, de veiligheid van medewerkers en bezoekers te borgen en de reputatie te beschermen. Het biedt een stelsel van maatregelen om de kritische bedrijfsprocessen onder crisisomstandigheden voort te zetten. De inrichting van het proces voor BCM is een lijnverantwoordelijkheid.

BCMM

De Belastingdienst gebruikt voor de implementatie van BCM het Business Continuity Maturity Model (BCMM®) van Virtual Corporation, Inc. dat structuur geeft aan de invulling van crisismanagement, bedrijfsherstel, technologieherstel en beveiligingsbeheer.

Onder BCM vallen:

- Business Continuity Management System (BCMS);
- Continuïteit en continuïteitsplannen;
- Crisismanagement en -plannen;
- Bedrijfshulpverlening (BHV) en ontruiming;
- Borging van BCM in de voortbrengingsprocessen.

Een BCMS is een systeem om business continuity vast te stellen, te implementeren, uit te voeren, te monitoren, te reviewen, te onderhouden en te verbeteren. Het omvat de organisatie(structuur), beleid, planningsactiviteiten, verantwoordelijkheden, procedures, processen en middelen. Het BCMS van de Belastingdienst maakt integraal onderdeel uit van het beveiligings-managementsysteem. De Belastingdienst heeft op corporate- en bedrijfsonderdeelniveau een BCMS.

Corporate BCMS

Het corporate BCMS bevat de uitkomsten van de BCMS-en op bedrijfsonderdeel niveau en kent de volgende documenten en producten:

- Corporate beleid voor bedrijfscontinuïteit (deze paragraaf B.1.2),
- Rollen, taken, verantwoordelijkheden en middelen;
- Rapportages en risicoanalyses die op basis van het BCMS van de bedrijfsonderdelen zijn opgesteld;
- Adviezen aan de CSO van de Belastingdienst.

Bedrijfsonderdeel BCMS

Het BCMS op bedrijfsonderdeelniveau omvat deze documenten en producten[7]:

- Beleid voor bedrijfscontinuïteit;
- Rollen, taken, verantwoordelijkheden en middelen;
- Definities voor bedrijfscontinuïteitsgerelateerde projecten;
- Voortgangsrapportage van bedrijfscontinuïteitsgerelateerde projecten;
- Registratie van trainingen en bekwaamheden;
- Uitkomsten van Business Impact Analyses;
- Dreigingsanalyses;
- Documenten die de gekozen strategieën verantwoorden;
- Beschrijving van het incidentproces;
- Incidentmanagement beschrijvingen;
- Plannen op operationeel, tactisch en strategisch niveau;
- Testprogramma's;
- Rapportages van oefeningen;
- Awareness- en trainingsprogramma's;
- Service level agreements met klanten en leveranciers (intern en extern),

[7] Conform de *Good Practice Guidelines 2013* van het Business Continuity Institute

- Contracten voor recovery services van externe partijen;
- Onderhouds- en review (audit) programma, rapportages en correctieve acties.

De documenten worden onderhouden aan de hand van periodieke audits die worden opgenomen in de reguliere auditplanning. In elk document is de onderhoudsperiode ervan vastgelegd.

B.1.2.1. Continuïteit

Kritische bedrijfsfuncties

De Belastingdienst heeft kritische bedrijfsfuncties benoemd op basis van de aan hem opgedragen wettelijke uitvoeringstaken, maar ook bijvoorbeeld op basis van impact en risico's op reputatieschade, maatschappelijke onrust of politieke invloed uit binnen- of buitenland. De keuze voor kritische functies die de Belastingdienst aan de hand van deze criteria heeft gemaakt is de volgende:

- Alle uitbetalingsprocessen naar burgers en/of bedrijven;
- Communicatiemiddelen naar burgers, bedrijven en eigen personeel;
- De stopfunctie[8] van Douane;
- Fysiek toezicht Douane;
- Vervoer Douane;
- Toeslagen.

Voor elke bedrijfsactiviteit van de Belastingdienst is vastgesteld wat de maximaal toelaatbare uitvalsduur (MTU) en het maximaal (toelaatbare) data verlies (MDV) is. Op basis hiervan moet bepaald zijn welke activiteiten als kritisch aangemerkt worden.

De Belastingdienst hanteert de volgende definities:

Crisis vs. calamiteit

- Een *calamiteit* is een onverwachte gebeurtenis met dusdanig negatieve gevolgen dat de reguliere probleemoplossende activiteiten onvoldoende zijn voor herstel van de normale situatie.
- Een *crisis* is een situatie waarbij de continuïteit van de bedrijfsvoering, de veiligheid van medewerkers (en bezoekers) en/of de reputatie van het bedrijf in gevaar is. Deze kan ontstaan door een calamiteit of een externe gebeurtenis. Bij een crisis wordt het crisismanagementteam geactiveerd.

In aanvulling hierop definieert de Belastingdienst kritische en risicovolle functies, zie paragraaf B.1.1.5.

B.1.2.2. Crisismanagement

Een crisissituatie kenmerkt zich door het niet toereikend zijn van de normale oplossingsmechanismen om een onverwachte gebeurtenis te bestrijden. Het crisismanagementteam neemt dan ook bij een crisis de besturing van de organisatie over. De besturingslijnen zijn kort en direct.

De crisisorganisatie van de Belastingdienst richt zich op de besturing van de organisatie tijdens een crisis en kent twee lagen van crisismanagement:

- De crisisteams van de (primaire) bedrijfsonderdelen managen de crisis;
- Het (concern)crisisteam van de Belastingdienst bestuurt deze teams in de gevallen waarbij er bedrijfsonderdeeloverstijgende keuzes gemaakt moeten worden.

[8] Onder andere onderdeel van de processen Fysiek toezicht, Binnenbrengen, Uitvoer en Toezicht reizigersbagage

Crisiscommunciatie

Eén van de belangrijkste aspecten van crisismanagement is de communicatie rond de crisis. Hiervoor hanteert de Belastingdienst de volgende principes:

Communicatieprincipes

- Crisiscommunicatie loopt organisatorisch gezien altijd van onder, naar boven, naar buiten;
- De crisiscommunicatie is te allen tijde gewaarborgd – er ligt een boodschap die in alle gevallen te gebruiken is;
- De boodschap is consistent ongeacht de persoon die of het kanaal dat deze brengt.

De inhoud van de boodschap in crisiscommunicatie wordt opgesteld door het crisisteam. De Directie Communicatie van Minfin/Cluster SG maakt deze inhoudelijke boodschap geschikt om via de verschillende kanalen (perswoordvoering, websites, social media, etc) verspreid te worden en geeft hier opdracht(en) voor.

Tevens zijn boodschappen voorbereid bij iedere vestiging of locatie van de Belastingdienst die in voorkomende gevallen gebruikt kunnen worden en zijn medewerkers geïnstrueerd hoe om te gaan met de media.

B.1.2.3. Continuïteitsstrategie

Enkelvoudige calamiteiten

Het BHV-plan, crisismanagementplan en de herstelplannen vormen tezamen het bedrijfscontinuïteitsplan. De Belastingdienst gaat bij calamiteitenscenario's uit van enkelvoudige calamiteiten.

Plannen

De plannen worden op corporate en op bedrijfsonderdeelniveau opgesteld. Elk bedrijfsonderdeel van de Belastingdienst beschikt over een actueel en periodiek getest plan:

- Complete crisismanagementplan tenminste één keer per jaar;
- Beschikbaarheid leden crisisteam tenminste één keer per kwartaal;
- Continuïteitsplan tenminste één keer per jaar;
- Evaluatie van de kritische bedrijfsactiviteiten één keer per jaar;
- Crisisteam tenminste één keer per jaar.

B.1.2.4. BHV en ontruiming

Lijnverantwoordelijkheid

Bedrijfshulpverlening en ontruiming worden bij de Belastingdienst ingevuld volgens de hiervoor geldende wettelijke kaders, aangevuld met de eventuele kaders van de Rijksoverheid. Bovendien kan de BHV-organisatie nadat de veiligheidstaken zijn uitgevoerd voor andere doeleinden ingezet worden door het (crisis)management. BHV en ontruiming en de werking hiervan is een lijnverantwoordelijkheid.

B.1.2.5. Fysieke uitwijk

Eigen gebouwen

In beginsel wordt er geen uitwijk buiten de Belastingdienstgebouwen voorzien. Uitwijk organiseren we binnen de eigen gebouwen, behoudens bijzondere situaties. Het betreft hier uitwijk ten behoeve van de continuïteit, niet voor (korte) opvang.

B.1.2.6. Borging van BCM in de voortbrenging

IV-keten

BCM-aspecten worden door middel van Methoden, Technieken, Hulpmiddelen en Voorschriften van de IV-keten geborgd zodat producten en processen voldoen aan het aan de bedrijfsprocessen gerelateerde niveau van BCM-eisen.

B.1.3. Beleid op toegang

Toegangs*beleid* is essentieel voor de veiligheid van medewerkers en bezoekers en voor de beveiliging van gegevens en goederen. Het begrip *toegang* omvat niet alleen de toegang van medewerkers tot kantoren en systemen maar ook de manieren van toegang van burgers, ondernemers, intermediairs en ketenpartners tot informatie en processen van onze organisatie.

Toegang tot informatie

Maatregelen op dit vlak zijn zowel fysiek als logisch van aard en worden als een geheel beschouwd en benaderd. Het principe hierbij is *vertrouwen voorop*, niet alleen in de eigen medewerker maar ook in burgers en bedrijven, samenwerkingsverbanden en ketenpartners. Tenslotte sluiten we met toegangsbeleid zoveel mogelijk aan bij ontwikkelingen zoals de Rijkspas en rijksoverheidsbreed identity management[9], DigiD en eID.

Beheer van identiteiten

Beveiliging is in sterke mate afhankelijk van het op orde zijn van identiteiten en autorisaties. Het beheren van (digitale) identiteiten en toekennen van autorisaties gebeurt daarom zoveel mogelijk geautomatiseerd en generiek voor alle systemen, waarbij overbodige autorisaties worden verwijderd en conflicterende autorisaties direct worden gesignaleerd zodat adequate maatregelen getroffen kunnen worden.

Toegangs*beheer* richt zich op het verlenen van toegang aan personen tot de gebouwen, de informatieverwerkende systemen, de gegevens die daarin worden verwerkt en opgeslagen en andere bedrijfsmiddelen. Het beheerproces beschermt deze gebouwen, systemen, gegevens en bedrijfsmiddelen tegen onbevoegde toegang, raadpleging, mutatie of oneigenlijk gebruik en houdt rekening met de verschillende toegangsbeveiligingsrollen (toegangsverzoek, -autorisatie en -administratie).

B.1.3.1. Beleid op fysieke toegang

Het fysieke toegangsbeleid is er op gericht om gebouwen en informatie te beschermen door ongeautoriseerde toegang te voorkomen. Het voorziet mogelijkheden voor het leveren van beveiligde ruimten, gecontroleerde omgevingen en beveiliging van bedrijfsmiddelen. Het draagt bij aan de veiligheid van groepen mensen en heeft verwantschap met de veiligheid van het individu (paragraaf B.1.10.1). Eén en ander wordt beschouwd vanuit de samenhang tussen risicoprofielen, zonering (rijksgebouwen, gemengde huisvesting), werkbaarheid en gedrag.

Fysieke veiligheid

CFD

Het tactisch beleid en de operationele realisatie van fysieke beveiliging is gedelegeerd aan en uitgewerkt[10] door het Belastingdienst/Centrum voor Facilitaire Dienstverlening.

Brede toegang

Belastingdienstmedewerkers hebben in principe toegang tot alle gebouwen van de Belastingdienst. Er zijn specifieke zones waar alleen geautoriseerd personeel mag komen. Gebouwen zijn ingericht volgens de rijksbrede normen voor zonering[11]. Zonering vervangt compartimentering op basis van organisatie(onderdelen), die niet meer wordt toegepast. Het management kan bewust van dit principe afwijken als daar gegronde redenen voor zijn.

[9] Programma Toegang, CIO Rijk/ICTU, maart 2013
[10] O m. Servicevisie Fysieke Beveiliging, CFD, 2013
[11] Zoneringsmodel rijkskantoren, Model voor beveiliging Te Beschermen Belangen, BZK/ICBR, juli 2011 en Normenkader Beveiliging Rijkskantoren (NkBR), BZK/RGD, februari 2013

Bijzonder werkgebied

Voor toegang tot het *bijzonder werkgebied* (zone 3) dient de specifieke richtlijn[12] van B/CFD te worden gebruikt.

Medewerker is geen bezoeker

Belastingdienstmedewerkers worden niet als bezoeker aangemerkt. Alleen aan niet-belastingdienstmedewerkers worden bezoekerspassen verstrekt. Aanmeldingen voor het "bezoek" van eigen medewerkers kunnen achterwege blijven, zij zijn ook onaangekondigd welkom in een gebouw. Hiermee lopen we gelijk op met de ontwikkeling van de Rijkspas en de toegang van rijksoverheidsambtenaren tot rijksoverheidsgebouwen en belastingdienstgebouwen[13].

Draagplicht

Het zichtbaar dragen van de Rijkspas draagt bij aan de personele veiligheid. Hiermee toont de drager/ster zichtbaar aan dat hij of zij in de basis is gelegitimeerd om zich in het gebouw te bevinden. Daarnaast wordt met een gepersonaliseerde pas de sociale controle versterkt ten opzichte het dragen van een anonieme bezoekerspas

B.1.3.2. Beleid op logische toegang

Autorisatieprofielen

Hierbij wordt op basis van *need-to-do* en *need-to-know* gewerkt (zie A.2, Beveiligingsprincipes). Eén en ander is vastgelegd in organisatiebrede en formeel vastgestelde autorisatieprofielen, aan de hand waarvan autorisaties worden toegekend. Hierbij passen we zoveel mogelijk organisatiebrede profielen toe (eenvoud van beheer).

Bij het beoordelen en ontwikkelen van beheersmaatregelen voor het proces van logisch toegangsbeheer worden de daartoe geldende richtlijnen[14] gevolgd.

B.1.3.2.1 Beleid op functiescheiding

Het scheiden van functies als onvervangbare basismaatregel voor een betrouwbare informatievoorziening volgt in principe de arbeidsverdeling van de organisatie. In hoofdlijnen worden processen gescheiden uitgevoerd. In het normenkader voor het basis beveiligingsniveau zijn daartoe overal in de verschillende processen gedetailleerde uitgangspunten opgenomen. Globaal gelden de volgende functiescheidingen:

- Tussen bewarende, registrerende, beslissende, uitvoerende en controlerende taken;
- Tussen beleid en uitvoering;
- Tussen gebruikersorganisatie en facilitaire organisatie: huisvesting (i.v.m. fysieke beveiliging) en levering van ICT;
- Tussen ontwikkeling en productie in leveren ICT;
- Met betrekking tot processen en ICT tussen functioneel, technisch en operationeel beheer.

Proces- en functiescheiding

Elk bedrijfsonderdeel heeft een eigen taak binnen de Belastingdienst en voert deze zelfstandig uit. Functiescheiding tussen de bedrijfsonderdelen behoort tot de standaard arbeidsverdeling. Binnen elk bedrijfsonderdeel is er functiescheiding tussen het primair en ondersteunend proces. Ook hier volgen we de standaard arbeidsverdeling.

Het ondersteunend proces omvat management, managementondersteuning en bedrijfsvoering (staf). Het primaire proces is per bedrijfsonderdeel verschillend

[12] Toegang tot het bijzonder werkgebied (zone 3) in Belastingdienstgebouwen, CFD, juni 2015.
[13] Beleid Toegang rijksambtenaren in Belastingdienstwerkruimten, CFD, 2013
[14] Rapport Beheersmaatregelen proces LTB v1 0, TBO, januari 2016

ingericht. Een standaard arbeidsverdeling voor een bedrijfsonderdeel ziet er bijvoorbeeld als volgt uit:

Management en staf – Heffing – Inning – Klantregistratie – Dienstverlening.

De functies *beschikken*, *bewaren*, *registreren*, *uitvoeren* en *controleren* moeten binnen elk proces gescheiden plaatsvinden. In termen van autorisaties betreft dit meestal de functies registreren en beschikken.

De functiescheiding wordt ondersteund door (procesgerichte) autorisatieprofielen. De profielen voor het primaire proces worden in hoofdgroepen ingedeeld en per hoofdgroep (Heffing, Inning etc.) in functionele muteer- en raadpleegprofielen.

De proceseigenaar beslist conform het (beveiligings)beleid uiteindelijk of een autorisatie door medewerkers van een ander proces kan worden gebruikt en stelt hieraan de noodzakelijke voorwaarden. Door dit vooraf al vast te stellen weet men bij voorbaat al welke speelruimte er is in situaties dat er vanuit een proces een verzoek om bijstand wordt gedaan.

In situaties dat een onderdeel van een proces elders uitgevoerd gaat worden spreken de (proces)eigenaren onderling af welke autorisaties over de processen heen ter beschikking worden gesteld.

B.1.3.2.2 Raadpleegrechten

Raadpleegrechten geven toegang tot gegevens. Je kunt de gegevens niet wijzigen of verwijderen. De beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens is gewaarborgd.

Vertrouwelijkheid wordt gewaarborgd door de medewerkers alleen die gegevens te laten raadplegen, die noodzakelijk zijn voor de uitvoering van taken, behorend bij een rol in het proces waarin ze werkzaam zijn volgens het principe van *need-to-know*. We brengen het te volgen principe en het uit te voeren beleid in beeld door procesgebonden raadpleegrechten te benoemen en deze binnen het proces functioneel te beleggen.

Need-to-know

Raadpleegrechten in het primaire proces kunnen, mits functioneel, over de processen heen in het raadpleegprofiel van een ander proces opgenomen worden.

B.1.3.2.3 Muteerrechten

Muteerrechten in het algemeen hebben invloed op de beschikbaarheid en integriteit van de gegevens. Het kunnen creëren, wijzigen en verwijderen van gegevens brengt risico's met zich mee op het gebied van de continuïteit van processen en de integriteit, beschikbaarheid en vertrouwelijkheid van de gegevens. Muteerrechten worden op basis van het principe *need-to-do* toegekend.

Need-to-do

Mutaties in de systemen van de Belastingdienst worden (in principe) altijd gelogd, waarbij de gegevens van de uitvoerend functionaris worden vastgelegd. Zorgvuldigheid is geboden bij het toekennen van muteerrechten, die een kritische functie binnen een proces vervullen.

Muteerrechten in het primaire proces worden binnen een bedrijfsonderdeel per hoofdproces functioneel ingedeeld. Een administratief medewerker bijvoorbeeld krijgt alleen de beschikking over muteerrechten, die noodzakelijk zijn voor het uitvoeren van de administratieve werkzaamheden. Hierbij wordt rekening gehouden met de functiescheidingsregels binnen het proces.