



Vertrouwelijk/Aangetekend
Ministerie van Financiën
Directoraat-Generaal Belastingdienst
T.a.v. de heer drs. P.H. Smink
Postbus 20201
2500 EE DEN HAAG

Datum

12 januari 2026

Ons kenmerk

2025-010112

Onderwerp

Onderzoek naar lokaal ontwikkelde applicaties bij de Belastingdienst

Geachte heer Smink,

In april 2024 heeft de Autoriteit Persoonsgegevens (AP) het toezicht op de Belastingdienst geïntensiveerd met als doel het realiseren van een duurzame verbetering van de bescherming van persoonsgegevens.¹ Een van de onderwerpen waarop dit geïntensiveerde toezicht zich richt betreft IT-applicaties die door de Belastingdienst gebouwd zijn buiten de daarvoor bestemde beleidskaders en waarin verwerkingen van persoonsgegevens plaatsvinden. Het gaat daarbij om zogeheten Lokaal Ontwikkelde Applicaties (LOA's) en Robuuste Tijdelijke Voorzieningen (RTV's). De Belastingdienst heeft honderden van dergelijke applicaties in werking. Deze applicaties zijn oorspronkelijk ontwikkeld buiten de kaderstelling van de Belastingdienst. Dat betekent dat deze applicaties onder andere op het gebied van privacy, informatiebeveiliging en bedrijfscontinuïteitmanagement niet altijd voldoen aan de (wettelijke) normen, zoals de AVG en de BIO. Daardoor brengt het bestaan en gebruik van LOA's en RTV's risico's met zich mee voor de rechten en vrijheden van burgers. Gelet op deze risico's heeft de AP een onderzoek uitgevoerd naar deze applicaties. In de bijlage van deze brief treft u het onderzoeksrapport aan waarin de resultaten van het onderzoek zijn opgenomen.

¹Brief van de voorzitter van de AP aan de Staatssecretaris van Fiscaliteit en Belastingdienst; 19 april 2024, Kenmerk 2024-28-AWO-GBU.

Datum
12 januari 2026

Ons kenmerk
2025-010112

Conclusie

De AP concludeert dat er onvoldoende gestuurd wordt op het laten voldoen van LOA's en RTV's aan de eisen van wet- en regelgeving op het punt van de bescherming van persoonsgegevens. Het ontbreekt aan eenduidig richtinggevend beleid, en aan toereikende centrale regie. Er is geen inzicht in de mate waarin de applicaties aan de wet- en regelgeving voldoen. Burgers lopen daardoor het risico dat er onzorgvuldig met hun persoonsgegevens wordt omgegaan, bijvoorbeeld doordat gegevens langer worden bewaard dan nodig, niet voldoende worden beveiligd, dat verouderde gegevens niet worden verwijderd of zelfs dat op basis van verouderde gegevens verkeerde beslissingen worden genomen.

De Belastingdienst streeft ernaar om LOA's terug te dringen. Daarbij ligt de nadruk op het terugdringen van LOA's welke worden gebruikt in primaire processen (zogenaamde bedrijfskritische LOA's). De verantwoordelijkheid om tot minder LOA's te komen ligt voor een groot deel bij de ketens en directies. Door de verantwoordelijkheid in overwegende mate bij de ketens en directies te beleggen, en deze verantwoordelijkheid onvoldoende te ondersteunen met een *duidelijke* kaderstelling vanuit de directie Informatievoorziening & databeheersing (IV&D) en een sterk gevoerde regie op de uitvoering van deze kaders, blijft de aanpak van LOA's diffuus, onoverzichtelijk en niet doelmatig. Dit terwijl juist het bestaan van LOA's binnen de verschillende ketens in 2024 is aangemerkt als een generiek probleem waarvoor een centrale aanpak voor de gehele Belastingdienst zou moeten worden ontwikkeld. De acties die in 2024 zijn ondernomen om dit probleem aan te pakken zijn echter inmiddels weer voor een groot deel verzand en gestrand.

In deze brief en bijlage werkt de AP deze conclusie nader uit, en wijst de AP op noodzakelijk te treffen maatregelen.

LOA's en RTV's

Binnen de bedrijfsprocessen van de Belastingdienst wordt een groot aantal applicaties gebruikt welke niet centraal worden beheerd door de directie Informatievoorziening. Dit soort applicaties noemt de Belastingdienst Lokaal Ontwikkelde Applicaties (LOA's). Omdat deze applicaties niet centraal worden beheerd is niet inzichtelijk hoeveel LOA's er zijn, waar ze voor worden gebruikt en of deze voldoen aan de kaders op onder andere het gebied van de AVG en BIO.

Applicaties die zijn ontstaan als LOA kunnen onder beheer worden gebracht bij de directie Informatievoorziening. Daarbij is het mogelijk dat de oorspronkelijke LOA wordt omgebouwd tot een reguliere applicatie welke aan de daarvoor door de Belastingdienst gestelde kaders voldoet. Het is echter ook mogelijk dat een LOA wordt omgebouwd naar een zogenaamde Robuuste Tijdelijke Voorziening (RTV). Dit is een LOA welke onder beheer is gebracht bij de directie Informatievoorziening, maar welke (nog) niet volledig aan de daarvoor gestelde kaders voldoet. Het gebruik van deze RTV's gaat derhalve mogelijk gepaard met vergelijkbare risico's voor burgers als bij het gebruik van LOA's.

Voornamelijk daar waar LOA's en RTV's worden gebruikt binnen de toezichtprocessen van de Belastingdienst bestaat het risico dat de rechten en vrijheden van burgers worden geschaad.

Datum

12 januari 2026

Ons kenmerk

2025-010112

Gelet op de hierboven genoemde risico's heeft de AP onderzoek uitgevoerd naar het bestaan en gebruik van LOA's en RTV's waarmee persoonsgegevens worden verwerkt binnen de Belastingdienst. Daarin werd in het bijzonder aandacht besteed aan LOA's en RTV's welke worden gebruikt in het toezicht op belastingplichtigen.

FSV (Fraude Signalering Voorziening) en RAM (Risico Analyse Model) zijn voorbeelden van LOA's uit het verleden. Met die systemen werden de rechten burgers in zeer ernstige mate geschaad, zoals ook blijkt uit eerdere publicaties van de AP. Die systemen zijn uitgezet. Een vigerende LOA met grote risico's is Informatiesjabloon, waarvoor de AP bij brief van 9 juli 2025 aan de Staatssecretaris van Fiscaliteit, Belastingdienst en Douane heeft verzocht om dat systeem op de kortst mogelijke termijn uit te faseren.

Beleid, inzicht en regie

De AP constateert dat de Belastingdienst geen centraal overzicht heeft van LOA's welke zich binnen de organisatie voordoen. Hierdoor kan niet worden vastgesteld hoe het aantal LOA's zich ontwikkelt. De AP oordeelt dat de centrale regie welke wordt gevoerd op de doelstelling om het aantal bedrijfskritische LOA's terug te dringen verder versterkt moet worden.

De AP concludeert verder dat er onvoldoende centrale regie wordt gevoerd op het laten voldoen van LOA's en RTV's aan de wet- en regelgeving. Er zijn geen richtinggevende kaders opgesteld om invulling te geven aan deze doelstelling.

Vanuit de ketens en directies zijn wel acties ondernomen ten aanzien van LOA's en RTV's, maar deze acties hebben geen systematisch en gestructureerd karakter en zijn niet gebaseerd op eenduidig Belastingdienst-breed beleid. De mate waarin deze acties succesvol zijn geweest is niet inzichtelijk gemaakt.

LOA's en RTV's voor toezicht: onderzoek naar 76 applicaties

De AP heeft 76 applicaties onderzocht welke konden worden geclassificeerd als LOA of RTV en welke naast het feit dat deze persoonsgegevens verwerken, ook worden gebruikt voor het toezicht op belastingplichtigen. Het vaststellen van de grondslag voor verwerking van persoonsgegevens en het vaststellen of deze verwerkingen voldoen aan het doelbindingsvereiste zijn essentieel om de rechtszekerheid en de voorspelbaarheid van de verwerking van persoonsgegevens voor burgers te waarborgen. Toch bleek uit dit onderzoek dat de vereiste grondslag en doelbinding niet voor alle verwerkingen welke gepaard gaan met het gebruik van LOA's en RTV's was vastgesteld. In 9% van de applicaties was de grondslag niet duidelijk, in 17% was niet vastgesteld of voldaan was aan het beginsel van doelbinding.

Over de exportmogelijkheden van deze applicaties concludeert de AP dat de Belastingdienst onvoldoende zicht heeft op welke gegevens mogelijk buiten de beveiligde omgeving van de organisatie terechtkomen. 65% van de onderzochte applicaties beschikte over een exportfunctie.

Daarnaast concludeert de AP dat voor de onderzochte applicaties weinig risicoanalyses waren uitgevoerd. Voor minder dan de helft van de applicaties was een risicoanalyse uitgevoerd in het kader van de

Datum
12 januari 2026

Ons kenmerk
2025-010112

bedrijfscontinuïteit. Ten aanzien van de mogelijke risico's voor belastingplichtigen bleek dat er nagenoeg géén systematische analyses waren uitgevoerd om mogelijke risico's in kaart te brengen en waar nodig te adresseren.

De AP ziet verder dat het autorisatiebeheer van deze applicaties niet in alle gevallen voldeed aan de daarvoor gestelde eisen. Logging en monitoring van gebruikersraadplegingen, een beveiligingsmaatregel die de risico's van een gebrekkig autorisatiebeheer kan adresseren, bleek nagenoeg niet te zijn geïmplementeerd.

Noodzakelijke maatregelen

Gelet op de risico's welke het gebruik van LOA's en RTV's die persoonsgegevens verwerken met zich mee kunnen brengen voor de rechten en vrijheden van belastingplichtigen, dient de Belastingdienst controle te krijgen over het gebruik en bestaan van deze applicaties. Gelet op de conclusies van dit rapport ziet de AP de noodzaak tot het treffen van de volgende maatregelen:

1. Toets in hoeverre vigerende LOA's en RTV's voldoen aan de AVG en de BIO en voer daar waar vereist risicoanalyses uit voor de verwerkingen welke worden uitgevoerd met deze applicaties.
2. Versterk de regie vanuit de directie IV&D. Draag daarbij zorg voor concrete kaders ten aanzien van het bestaan en gebruik van LOA's en RTV's. Zorg voor een centraal overzicht van (bedrijfskritische) LOA's op basis waarvan kan worden gestuurd op de doelstelling om het bestaan van deze applicaties terug te dringen.
3. Stel een plan op waaruit blijkt hoe en binnen welke termijn LOA's en RTV's moeten worden omgezet in reguliere applicaties, en voer dat plan vervolgens uit. Werk daarin ook uit in welke situaties een LOA of RTV moet worden stopgezet.
4. Beperk de mogelijkheden tot gegevensleveringen uit bestaande bronsystemen aan LOA's zodat het ontstaan van (bedrijfskritische) LOA's wordt teruggedrongen. Zorg ervoor dat nieuwe bedrijfskritische LOA's uitsluitend ontstaan als dit volgens een lid van het bestuursteam dringend noodzakelijk is bevonden en mits deze voldoen aan daaraan te stellen eisen.

De conclusies en aanbevelingen uit deze brief worden nader uitgewerkt in bijgevoegd onderzoeksrapport.

Tot slot

Voorkomen moet worden dat LOA's en RTV's worden beschouwd als een noodzakelijke en acceptabele tussenstap die vervolgens vele jaren voortduurt. Het besef moet doordringen dat wanneer een LOA of RTV niet aan de regelgeving voldoet ten aanzien van de bescherming van persoonsgegevens dit ernstige risico's met zich meebrengt, en dat deze risico's moeten worden geadresseerd aan de hand van noodzakelijk te treffen maatregelen.

De AP verzoekt de Belastingdienst dan ook dringend om bovenstaande maatregelen uit te voeren. De AP zal elk halfjaar de voortgang van de nakoming van de maatregelen monitoren. Daartoe verzoekt de AP de Belastingdienst om elk halfjaar een rapportage toe te zenden met daarin de stand van zaken per maatregel. Op basis van die rapportage gaat de AP het gesprek met u aan.

**Datum**

12 januari 2026

Ons kenmerk

2025-010112

Een kopie van deze brief zal worden verzonden aan uw Functionaris voor Gegevensbescherming (FG).

Deze brief wordt op 28 januari 2026 op de website van de AP gepubliceerd.

Met vriende¹ ●●

Autoriteit

mr. drs. G.N.J. u w= u, 
Programmadirecteur



AP

bescherming in een
digitale wereld

Onderzoeksrapport

Lokaal ontwikkelde applicaties bij de Belastingdienst

12 januari 2026

Inhoudsopgave

Inhoudsopgave	2
1. Applicaties gebouwd buiten de kaders	4
1.1 Inleiding	4
1.2 LOA's en RTV's	4
1.3 Risico's van LOA's en RTV's	6
1.4 Opzet van het onderzoek	6
2. Overzicht van applicaties	9
3. Beleid inzake LOA's en RTV's	11
3.1 Inleiding	11
3.2 Beleid	11
3.3 Uitvoering van het beleid	12
4. Regie op terugdringen LOA's	13
4.1 Rol IV&D	13
4.2 Rol adoptieouder	13
4.3 Sturing door directies zelf	14
4.4 Conclusie	15
5. LOA's en RTV's voor toezicht	16
5.1 Inleiding	16
5.2 Persoonsgegevens en grondslag	17
5.2.1 Welke persoonsgegevens	17
5.2.2 Grondslag	17
5.2.3 Doelbinding	18
5.2.4 Exportfunctie	19
5.2.5 Verstrekking aan andere organisaties	19
5.2.6 Bewaren van gegevens	20
5.3 Risicoanalyses	20
5.3.1 Risicoanalyses voor betrokkenen	21
5.3.2 Risicoanalyses bedrijfscontinuïteit	22
5.4 Beveiliging	22
5.4.1 Autorisatiebeheer	23
5.4.2 Loggen en monitoren van de gebruikersactiviteiten	24
5.4.3 Maken van een back-up van de applicatie	25
6. Conclusies en noodzakelijke maatregelen	26
6.1 Inleiding	26
6.2 Samenvatting conclusies	26
6.2.1 Beleid, inzicht en regie	26
6.2.2 LOA's en RTV's voor toezicht	26



6.3	Overkoepelende conclusies	27
6.4	Noodzakelijke maatregelen	28
6.4.1	Noodzakelijke maatregelen ten aanzien van LOA's en RTV's	28
6.4.2	Toets LOA's en RTV's aan de AVG en de BIO en voer daar waar vereist risicoanalyses uit	28
6.4.3	Kaders, regie en overzicht	29
6.4.4	Een plan om LOA's en RTV's uit te faseren	29
6.4.5	Beperk gegevensleveringen uit bronsystemen	30

1. Applicaties gebouwd buiten de kaders

1.1 Inleiding

Bij de Belastingdienst zijn honderden applicaties in gebruik die zijn ontwikkeld door medewerkers die werkzaam zijn op diverse belastingkantoren in het land. Deze applicaties zijn veelal ontwikkeld omdat ze voorzien in een dringende behoefte voor het dagelijkse werk op de werkvloer. De applicatie leidt bijvoorbeeld tot efficiënter werken, of is behulpzaam bij het maken van berekeningen voor op te leggen aanslagen. Doordat de IV-portfolio bij de Belastingdienst overvol is, concurreert de wens voor een specifieke applicatie die wél aan alle eisen voldoet met vele andere prioriteiten. Daardoor kan het bouwen van de gewenste volwaardige applicatie een zeer lange tijd duren. Politieke wensen ten aanzien van de IV-portfolio gaan daarbij vaak voor.

Wanneer er met deze applicaties verwerkingen van persoonsgegevens worden uitgevoerd is hierop de AVG van toepassing. De AVG beschermt de grondrechten en fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens. De verwerkingen van persoonsgegevens die met het gebruik van de voornoemde applicaties plaatsvinden zullen dan ook dienen te worden uitgevoerd in lijn met deze beginselen en bepalingen. Kenmerkend voor deze applicaties is echter dat ze zijn ontwikkeld buiten de kaderstelling van de Belastingdienst op het gebied van privacy, informatiebeveiliging en bedrijfscontinuïteitmanagement. Daardoor brengt het bestaan en gebruik van deze applicaties risico's met zich mee voor de rechten en vrijheden van burgers.

Gelet op deze risico's heeft de AP een onderzoek uitgevoerd naar LOA's (Lokaal Ontwikkelde Applicaties) en RTV's (Robuuste Tijdelijke Voorzieningen) die worden gebruikt binnen de Belastingdienst en die persoonsgegevens verwerken.

1.2 LOA's en RTV's

LOA's voorzien in kleinschalige- en incidentele automatiseringsvragen en worden met lokale ontwikkelcapaciteit bij de eenheden ontwikkeld en onderhouden. In veel gevallen wordt hiervoor standaard kantoorsoftware toegepast.¹ LOA's worden meestal gebouwd in Access of Excel. Ze worden formeel niet beheerd en onderhouden door de directie IV.

In 2023 is in het zogeheten memo Technische schuld bepaald dat de plek waar het *beheer* en het *onderhoud* plaatsvinden relevant is voor de vraag of een applicatie een LOA is of niet. Tot dat moment was de plek van de *ontwikkeling* bepalend voor de vraag of een applicatie een LOA is.²

LOA's mogen geen bedrijfskritisch karakter hebben. Van een bedrijfskritisch karakter is sprake als de uitvoering van een bedrijfsproces niet goed mogelijk is zonder deze LOA. LOA's met een bedrijfskritisch

¹ Nota beleidsrichting LOA's versie 0.96 (2010).

² Memo Technische Schuld, Concerndirectie IV&D, 8 december 2023. Het memo is ingediend bij de Concern Architectuur Board Belastingdienst.



karakter moeten worden omgezet naar een Robuuste Tijdelijke Voorziening (RTV), of naar een Reguliere Voorziening.

Schaduw-IT omvat alle vormen van hard- of softwaregebruik zonder dat de organisatie hier weet van heeft, betrokken bij is geweest of toestemming voor heeft gegeven.³ LOA's kunnen getypeerd worden als schaduw-ICT en vallen daarmee per definitie buiten het domein van de ICT-voorziening waar de Belastingdienst in control over is.

Een RTV is in beheer en onderhoud bij de directie IV. Een RTV heeft een bewust tijdelijk karakter die op het moment van realisatie (of adoptie) om dan vigerende redenen (nog) niet voldoet aan de kaderstelling vanuit architectuur- en/of het technologiekader-IV. Aan een RTV moet een houdbaarheidsdatum worden gehangen.

Een RTV is derhalve een applicatie waarvan tijdelijk wordt toegestaan dat deze afwijkt van de kaders welke binnen de organisatie voor informatievoorziening zijn vastgesteld. Het proces waarbinnen een RTV gaat voldoen aan deze kaders en daarmee dus een reguliere applicatie wordt beslaat vaak meerdere jaren.⁴ De functionaliteit van een RTV kan dus nog steeds hetzelfde zijn als op het moment dat deze applicatie als LOA werd gebruikt buiten de architectuur. Als de LOA op functioneel gebied derhalve niet voldeed aan de kaders, dan bestaat de kans dat de omzetting naar RTV hier niet direct verandering in brengt.

RTV's zijn in beheer bij de afdeling LIV van de directie IV. Vertegenwoordigers van die afdeling zijn het overigens inhoudelijk niet eens met de definitie van een LOA die hierboven is genoemd, en die door het CTO-office wordt gehanteerd.⁵ De afdeling LIV ziet een RTV als een applicatie die gebouwd is met moderne technologie en die in beheer en onderhoud is bij de directie IV, en waarvoor de formele architectuurkaders gelden. Applicaties die draaien op een end of life c.q. verouderde technologie en zijn ondergebracht bij IV ziet LIV niet als RTV's, maar als LOA's. De achterliggende gedachte achter het maken van dit inhoudelijk onderscheid zit in de risico's welke deze end of life technologieën met zich meebrengen in het kader van bedrijfscontinuïteitmanagement. Met het hanteren van de definitie van het CTO-office zijn deze inhoudelijke verschillen tussen de beheerde applicaties niet langer inzichtelijk. De afdeling LIV hanteert derhalve feitelijk een andere definitie (namelijk een definitie gebaseerd op 'type technologie') dan opgenomen in het memo Technische schuld (namelijk 'plek waar beheer en onderhoud plaatsvinden').

De AP heeft in gesprekken met vertegenwoordigers van de directies CAP, MKB, GO en P gevraagd naar de definitie van een LOA en een RTV. Opvallend was dat er geen eenduidig beeld was van de definities.

De AP concludeert dat er geen eenduidige definitie van LOA's en RTV's is aangetroffen die geldt voor de hele dienst, en waarover overeenstemming bestaat.

³ <https://www.digitaltrustcenter.nl/schaduw-it>

⁴ Hoewel de Belastingdienst ernaar streeft om een RTV na drie jaar om te zetten naar een reguliere applicatie, wordt deze termijn vaak overschreden.

⁵ Verslag gesprek AP/Afdeling LIV, 5 februari 2025.

1.3 Risico's van LOA's en RTV's

De volgende risico's zijn verbonden aan LOA's:⁶

- Applicaties zijn niet ingericht volgens de principes van privacy-by-design;
- Ongeautoriseerde toegang tot bestanden en daarmee persoonsgegevens is mogelijk;
- Ongeautoriseerde wijzigingen van bestanden en daarmee van persoonsgegevens is mogelijk;
- De datakwaliteit kan niet worden gegarandeerd;
- Er zijn vaak te ruime mogelijkheden tot het exporteren van gegevens;
- Er is onvoldoende nagedacht over de vereiste grondslag en doelbinding en andere aspecten van de AVG;
- Applicaties worden ingericht naar eigen inzicht van individuele medewerkers, buiten de vastgestelde eisen van de reguliere IV om;
- Overmatige afhankelijkheid van niet-reguliere IV in het primaire proces;
- Applicaties vallen buiten het systeem van reguliere interne controles en interne audits, en blijven buiten het zicht van auditoren en (externe) toezichthouders;
- Er is geen of gebrekkige documentatie beschikbaar;
- De applicatie is niet getoetst aan de eisen vanuit informatiebeveiliging;
- Gemaakte wijzigingen in LOA's worden onvoldoende getest en gedocumenteerd.

LOA's zijn door de Belastingdienst in juli 2024 als een 'hoog risico gap' geïdentificeerd.⁷ Dit impliceert dat de Belastingdienst onderkende dat er geen registratie was van LOA's en dat veel LOA's niet compliant waren aan de AVG en/of de BIO. Ze zijn niet opgenomen in de domeinarchitectuur. Bij 'hoog risico gaps' gaat het onder meer om de risico's voor de burger.

De risico's van RTV's zijn in beginsel beperkter, want deze vallen onder het beheer van de directie IV. De beveiligingsmaatregelen zijn veelal sterker dan bij LOA's. Verder zijn voor LOA's in het algemeen geen maatregelen geïmplementeerd die een vastgesteld niveau van beschikbaarheid garanderen. Voor applicaties die door de directie IV worden beheerd, zijn daarentegen wel altijd waarborgen geïmplementeerd om een afgesproken niveau van beschikbaarheid te garanderen.

Applicaties kunnen de volgende levenscyclus doormaken: starten als een LOA (fase 1), na een bepaalde periode worden omgezet in een RTV (fase 2), en vervolgens worden opgenomen in de reguliere domeinarchitectuur (fase 3). Elke stap in deze levenscyclus kan lang duren, vanwege de grote uitdagingen in het IV-portfolio van de Belastingdienst. De risico's op het punt van de bescherming van persoonsgegevens en informatiebeveiliging worden in beginsel met elke stap beperkter. Deze applicaties kunnen natuurlijk ook in elke fase worden uitgezet of uitgefaseerd.

1.4 Opzet van het onderzoek

Het onderzoek van de AP ziet op LOA's en RTV's waarmee verwerkingen van persoonsgegevens worden uitgevoerd. De AP heeft in de periode van januari – december 2025 diverse gesprekken gevoerd met

⁶ Een aantal van deze risico's is ook genoemd in het document 'AVG richtlijnen LOA's' (datum: onbekend, waarschijnlijk 2024).

⁷ Brief van de directeur IV&D aan de AP, 10 januari 2025, kenmerk 2025-0000002603.



functionarissen van de Belastingdienst. Het gaat om gesprekken met datacoördinatoren, business analisten, business security officers, solution architecten, medewerkers van de Afdeling LIV, de adoptieouder voor LOA's, de CDO en medewerkers architectuursturing/voortbrengingsproces. Medewerkers van de CPO-office waren bij de gesprekken aanwezig.

De AP heeft daarnaast diverse documenten opgevraagd, waaronder overzichten van LOA's en RTV's en beleidsdocumenten.

Verder heeft de AP een vragenlijst opgesteld voor LOA's en RTV's die persoonsgegevens verwerken en die in aanvulling daarop worden ingezet voor het toezicht op belastingplichtigen, zoals uitgevoerd door de Belastingdienst. Hierbij dient te worden gedacht aan applicaties die erop gericht zijn om informatie voor het toezicht te analyseren, overzichtelijk weer te geven, selecties te maken, prioriteiten te stellen, planningen te maken voor de inzet van inspecteurs, rapporten te genereren, besluiten voor te bereiden enzovoorts. De Belastingdienst is verzocht om voor applicaties die persoonsgegevens verwerken en worden ingezet voor het toezicht vragenlijsten in te vullen.

De AP heeft in eerste instantie 92 vragenlijsten ontvangen. Uiteindelijk bleken 76 vragenlijsten daadwerkelijk persoonsgegevens te bevatten én te worden ingezet voor het door de Belastingdienst uitgevoerde toezicht op belastingplichtigen.

Een deel van de vragenlijsten was overigens slecht ingevuld. Geregeld waren vragenlijsten grotendeels niet ingevuld, of waren de vragen niet consequent ingevuld. Dat gold vooral voor de directie IV, en voor de keten Inkomensheffing. De AP heeft gelet op de imperfecties in de beantwoording de ketens en directies verzocht om de vragenlijsten te controleren op volledigheid en juistheid, en daar waar nodig aan te vullen. Daarvoor hebben de ketens en directies zeven weken extra de tijd gekregen (juli en augustus 2025).

De AP vraagt zich overigens af of de Belastingdienst volledig is geweest met het aanleveren van de verzochte informatie. Het is de AP opgevallen dat er meer dan 100 selectie-instrumenten zijn bij de Belastingdienst, die gebruikt worden in het toezicht van de Belastingdienst. Het aantal van 100 is aangedragen door de Belastingdienst in het kader van het project 'Discriminatie/selectieinstrumenten' dat de AP gelijktijdig aan het onderhavige project uitvoerde. Bij in elk geval zeven selectie-instrumenten heeft de AP het sterke vermoeden dat sprake is van een LOA. Dit omdat het selectie-instrument een Excel bestand betreft, of omdat de Belastingdienst heeft aangegeven dat het betreffende selectie-instrument 'nog wordt opgenomen in de domeinarchitectuur'.

De AP heeft de Belastingdienst in oktober 2025 gevraagd of de selectie-instrumenten ook LOA's kunnen zijn. Daarop heeft de Belastingdienst aangegeven dat het waarschijnlijk is dat er selectie-instrumenten zijn die als LOA zijn te karakteriseren.

Derhalve moet geconcludeerd worden dat de Belastingdienst niet volledig is geweest in het aanleveren van de verzochte informatie over LOA's die in het toezicht worden gebruikt. Ook voor dergelijke LOA's hadden vragenlijsten moeten worden ingevuld.

Om het onderhavige project niet te vertragen, en de Belastingdienst in staat te stellen om gesignaleerde risico's uit dit onderzoek zo snel mogelijk te adresseren, heeft de AP ervoor gekozen het onderzoek af te ronden op basis van de 76 ingevulde vragenlijsten.



Gelet op het bovenstaande wijst de AP nogmaals op het belang van een volledig en actueel verwerkingsregister. De verwerkingen van persoonsgegevens die binnen LOA's plaatsvinden zullen in elk geval in het verwerkingsregister terug moeten komen. De AP heeft niet onderzocht of dat op dit moment het geval is.

2. Overzicht van applicaties

In dit hoofdstuk staat de vraag centraal hoeveel LOA's en RTV's er zijn en of de Belastingdienst beschikt over een totaaloverzicht van de LOA's en RTV's die bij de dienst in gebruik zijn.

De AP constateert dat de Belastingdienst niet beschikt over een betrouwbaar totaaloverzicht.

De AP heeft daarom begin 2025 aan de directies gevraagd hoeveel LOA's en RTV's zij in gebruik hebben bij ketens/directies. Dat leverde geen eenduidig overzicht op. Op basis van de verstrekte overzichten schat de AP in dat er ongeveer 450 LOA's en RTV's bij de Belastingdienst in gebruik zijn. De meeste applicaties zijn in gebruik bij de directie Grote Ondernemingen en de daaraan verbonden ketens (volgens opgave: circa 285). De minste applicaties zijn in gebruik bij de directie Particulieren en de daaraan verbonden ketens (volgens opgave: 20).

De Belastingdienst maakt onderscheid tussen bedrijfskritische LOA's en niet bedrijfskritische LOA's. Bedrijfskritische LOA's moeten opgenomen zijn in de architectuurrepository. Niet bedrijfskritische LOA's *mogen* worden opgenomen als de domeinarchitect van de desbetreffende domeinarchitectuur dat relevant acht voor de architectuursturing. In de architectuurrepository staan 282 actieve LOA's (exclusief FIOD, Douane en Toeslagen). 149 LOA's hebben volgens opgave van de ketens een bedrijfskritisch karakter.

Er bestaan meer niet-bedrijfskritische LOA's dan opgenomen in de architectuurrepository. Omdat er geen afgebakende grens is tussen LOA's en bijvoorbeeld 'gewone' Excel-spreadsheets is het lastig om exact te vast te stellen hoeveel niet-bedrijfskritische LOA's er zijn. De Belastingdienst zelf geeft aan dat dit onmogelijk is.

Uit het overzicht van bedrijfskritische LOA's opgenomen in de architectuurrepository blijkt dat er vooral veel bedrijfskritische LOA's zijn bij de ketens Inning & Betalingsverkeer (48)⁸, Gegevens (43) en Bedrijfsvoering (30).

De CDO gaf in december 2025 in gesprek met de AP aan dat er acties lopen om de administratie van bedrijfskritische LOA's verder op orde te brengen. Deze acties worden in het eerste kwartaal van 2026 afgerond.

Aan bedrijfskritische LOA's moet in de architectuurrepository een werkpakket gekoppeld worden dat gericht is op vervanging/overdracht/uitfasering van de LOA. Aan bijna 90% van de LOA's is blijkens de administratie zo'n werkpakket gekoppeld. Blijkens dat overzicht worden bedrijfskritische LOA's uitgefaseerd verspreid over de jaren 2025 – 2029. Voor 10% van de LOA's is echter nog geen datum genoemd. Als wel een datum genoemd is, is daadwerkelijke uitfasering overigens afhankelijk van de prioritering in de IV-portfolio. De huidige situatie is dat de portfolio van de Belastingdienst overvol is, waardoor dit type werkpakketten regelmatig wordt uitgesteld, om ruimte te maken voor projecten die urgente continuïteitsrisico's mitigeren of (fiscale) wet- en regelgeving implementeren.

⁸ De keten Inning & Betalingsverkeer had zijn bedrijfskritische LOA's in december 2025 nog niet allemaal in de architectuurrepository staan (wel op een separate lijst). De repository wordt aangevuld.



De AP concludeert dat de Belastingdienst niet beschikt over een eenduidig overzicht van het aantal LOA's en RTV's dat bij de dienst in gebruik is. Er is wel inzicht in bedrijfskritische LOA's, maar ook daarvan is de administratie nog niet geheel op orde. Het is daardoor lastig om vast te stellen hoe het aantal (bedrijfskritische) LOA's zich ontwikkelt in de tijd.

3. Beleid inzake LOA's en RTV's

3.1 Inleiding

In dit hoofdstuk staat de vraag centraal welk beleid de Belastingdienst voert ten aanzien van LOA's en RTV's, en wat de stand van zaken is van de uitvoering van dat beleid.

3.2 Beleid

Alle toepassingen binnen de Belastingdienst, dus ook LOA's en RTV's, dienen te voldoen aan wet- en regelgeving op het vlak van de bescherming van persoonsgegevens en informatiebeveiliging. Voor de bescherming van persoonsgegevens zijn met name de AVG en de Richtlijn Gegevensbescherming bij Rechtshandhaving (RGR) van belang. Voor de eisen ten aanzien van informatiebeveiliging zijn vooral de BIO (Baseline Informatiebeveiliging Overheid), de NIS 2 (Network Information Security 2) en de CRA (Cyber Resilience Act) relevant. De eisen ten aanzien van de AVG en de BIO komen terug in de Referentiearchitectuur Integrale Beveiliging (Q1 2020).⁹

De AP heeft beleid opgevraagd ten aanzien van het bestaan van LOA's, de eisen die daaraan gesteld moeten worden en het terugdringen van LOA's. In de Referentiearchitectuur Integrale Beveiliging (Q1 2020) zijn geen passages opgenomen over het bestaan van LOA's en de (on)wenselijkheid daarvan. Ook zijn in de Referentiearchitectuur geen teksten opgenomen waaruit expliciet blijkt dat LOA's moeten worden teruggedrongen, en hoe dat wordt aangepakt. Evenmin wordt geëxpliciteerd dat de in eerste alinea van deze paragraaf genoemde eisen ook gelden voor LOA's en RTV's. De AP heeft geen vastgesteld beleid aangetroffen dat voor de hele Belastingdienst geldt.

Wel zijn vanuit enkele ketens beleidstukken aangedragen, waarvan de status echter veelal onduidelijk is. Meestal gaat het om conceptstukken, met nog allerlei markeringen in de tekst. Voor twee organisatie-eenheden is een vastgesteld document aangetroffen. Voor SSO F&MI is een vastgesteld document aangetroffen met de titel: *"LOA beleid Team Middelenaanadministratie en Financiële Verantwoording"*.¹⁰ Vanuit CAP is een vastgesteld document aangetroffen met de titel *'AVG richtlijnen bij de inzet van een LOA'*.¹¹

In de verschillende (concept)beleidsdocumenten die de AP heeft ontvangen zijn enkele rode draden af te leiden:

- LOA's worden als ongewenst gekarakteriseerd. De risico's van de LOA's worden uitgewerkt.
- Aangegeven wordt dat het belangrijk is erop toe te zien dat de LOA's die er nog zijn "zo veel als mogelijk en zo veilig en verantwoord mogelijk gebruikt worden". De richtlijnen zijn met dat doel opgesteld.
- Uitgangspunt is dat LOA's geen bedrijfskritisch karakter mogen hebben. Het uitvallen van een LOA mag geen onoverkomelijke problemen opleveren voor het uitvoeren van de processen van de Belastingdienst.

⁹ Versie Q1 2020, 23-03-2020. Vastgesteld in het MT van de Belastingdienst van 18-06-2020

¹⁰ Dit is vastgesteld in het MT SSO F&MI van 20-2-2023.

¹¹ Onduidelijk is wanneer het document is vastgesteld.



- Belangrijke elementen uit de AVG worden genoemd, en er worden praktische stappen genoemd waaruit blijkt wat er moet gebeuren om een LOA aan de AVG te laten voldoen.

Uit de in het kader van dit onderzoek gevoerde gesprekken leidt de AP af dat de Belastingdienst ernaar streeft het aantal LOA's terug te dringen. Het gaat daarbij in elk geval om LOA's die bedrijfskritisch zijn. Het gebruik daarvan moet worden gestopt. Niet geheel duidelijk is of LOA's die niet bedrijfskritisch zijn ook moeten worden teruggedrongen, of dat deze mogen blijven bestaan. Impliciet lijkt uit de stukken en de gesprekken te blijken dat LOA's die niet bedrijfskritisch zijn tijdelijk worden gedoogd, maar dat ze uiteindelijk ook moeten worden omgezet in een Reguliere Applicatie. Een duidelijke beleidslijn op dat punt heeft de AP evenwel niet aangetroffen.

Het beleid ten aanzien van RTV's is dat deze binnen 3 jaar moeten worden omgebouwd tot een Reguliere Applicatie.¹²

3.3 Uitvoering van het beleid

De Belastingdienst heeft geen goed inzicht in de ontwikkeling van het aantal LOA's binnen de dienst. Niet bekend is bijvoorbeeld hoeveel LOA's de laatste jaren zijn gestopt of omgezet in RTV's of in Reguliere Applicaties. Niet vastgesteld kan worden of de gewenste daling van het aantal LOA's ook daadwerkelijk wordt gerealiseerd.

Evenmin heeft de Belastingdienst inzicht in de vraag in hoeverre de nog in gebruik zijnde (bedrijfskritische) LOA's voldoen aan de eisen ten aanzien van de bescherming van persoonsgegevens en informatiebeveiliging. Audits op dit punt zijn niet aangetroffen.

Uit gesprekken met de directies P en MKB is overigens wel gebleken dat er in 2024 diverse LOA's zijn omgezet in RTV's. Exacte aantallen zijn niet aangetroffen.

¹² Gesprekverslag AP/LIV, 5 februari 2025.

4. Regie op terugdringen LOA's

4.1 Rol IV&D

Gelet op de taak van de directie Informatievoorziening & Databeheersing (IV&D) ten aanzien van processen en systemen binnen de Belastingdienst, zou het logisch zijn als er vanuit deze directie richtinggevende kaders worden opgesteld om de gap ten aanzien van LOA's aan te pakken. Zo zou er uitgewerkt kunnen worden aan welke eisen LOA's en RTV's moeten voldoen gedurende de periode dat ze nog niet zijn uitgezet of omgezet naar de reguliere domeinarchitectuur. De AP heeft een dergelijke aanpak niet aangetroffen. De directie IV&D voert niet de regie op het laten voldoen van LOA's aan wet- en regelgeving. Richtinggevende kaders ten aanzien van deze doelstelling zijn niet beschikbaar. De verantwoordelijkheid om LOA's te laten voldoen aan wet- en regelgeving is voor het overgrote deel belegd bij de afzonderlijke ketens.

Ten aanzien van de doelstelling om het aantal LOA's welke zijn geclassificeerd als bedrijfskritisch terug te dringen wordt wel een zekere mate van regie gevoerd door de directie IV&D. Deze bedrijfskritische LOA's dienen te worden opgenomen in de architectuur van de Belastingdienst. Voor zover deze applicaties niet voldoen aan de daarin gestelde kaders, dient bij opname in deze architectuur door de domeinarchitecten te worden aangegeven wanneer deze afwijkingen ten opzichte van de kaders worden opgelost door middel van zogenaamde werkpakketten.

Vanuit IV&D zijn domeinarchitecten gedetacheerd bij de ketens. De ketens dienen jaarlijks hun domeinarchitectuur goed te laten keuren, waarin ook wordt nagegaan in hoeverre bedrijfskritische LOA's zijn opgenomen in deze architectuur en of bij deze opname is aangegeven wanneer en op welke wijze de bij de LOA's behorende afwijkingen worden opgelost aan de hand van een werkpakket.

Door middel van deze architectuurssturing wordt er ten aanzien van LOA's welke als bedrijfskritisch zijn geclassificeerd een zekere mate van regie gevoerd op de doelstelling om deze terug te dringen. Hierbij dient de kanttekening te worden geplaatst dat LOA's welke niet als bedrijfskritisch zijn geclassificeerd met deze aanpak buiten beschouwing blijven.¹³ Ook in die LOA's kunnen persoonsgegevens worden verwerkt.

4.2 Rol adoptieouder

In het laatste kwartaal van 2024 is het zogeheten sponsors overleg in het leven geroepen. Doel van dit overleg is om te komen tot een gezamenlijke aanpak van de hoog risico gaps die organisatie breed in meerdere ketens voorkomen. Iedere vertegenwoordigende keten heeft een gap-thema 'geadopteerd' om tot een generieke aanpak voor de hoog risico gaps te komen.¹⁴ Voor iedere generieke gap is een adoptieouder aangesteld. Zo is er ook een adoptieouder aangesteld om de gap ten aanzien van LOA's aan te pakken. Deze adoptieouder zorgt ervoor dat handvaten worden aangereikt om de gap ten aanzien van de

¹³ In gesprekken met de Belastingdienst is aangegeven dat het domeinarchitecten ook is toegestaan om niet bedrijfskritische LOA's op te nemen in de domeinarchitectuur. Dit is echter niet verplicht.

¹⁴ Brief van de directeur IV&D aan de AP, 10 januari 2025, kenmerk 2025-0000002603.



LOA's op te lossen. Het daadwerkelijk oplossen van de gaps is echter de verantwoordelijkheid van de ketens zelf.

De adoptieouder voor LOA's heeft in juli 2024 een plan opgesteld met als titel "AVG risico's bij inzet en gebruik LOA's".¹⁵ Dit plan omvat een aantal stappen:

- Alle lopende initiatieven binnen de directies van de keten in beeld brengen;
- Inrichten van overkoepelende aansturing vanuit keten inzake opzet en bestaan;
- In beeld brengen van LOA's die bedrijfskritisch zijn;
- Bedrijfskritische LOA's in Domeinarchitectuur onderbrengen;
- Inventariseren per dienstonderdeel of beleid binnen dienstonderdeel aanwezig is en wordt nageleefd;
- Richtlijnen opstellen 'gebruik LOA's';
- Implementeren en/of naleven beleid 'gebruik LOA's'.

De AP vindt dit een verstandig stappenplan. De ketens zijn evenwel vrij om dit stappenplan te volgen en mogen afwijken van centraal opgestelde plannen.¹⁶ Dat past bij de wijze waarop de verantwoordelijkheid binnen de Belastingdienst is belegd.

De adoptieouder heeft geen doorzettingsmacht om de gap ten aanzien van de LOA's aan te pakken en op te lossen. Zij initieert de besluitvorming in de daarvoor bestemde gremia over de kaders en handvaten. Zij heeft niet tot taak om te monitoren of de besluiten Belastingdienst breed worden uitgevoerd.

De adoptieouder heeft derhalve geen zicht op de stand van zaken van de uitvoering van het plan, Belastingdienst breed.

De AP concludeert dat de verantwoordelijkheid voor het oplossen van de gap LOA's volledig bij de ketens ligt, en dat ketens vrij zijn om de gap op de voorgestelde manier aan te pakken. Er is een grote mate van vrijblijvendheid. De rol van de adoptieouder in het oplossen van de gap Belastingdienst breed is beperkt tot aanjagen en initiëren. De AP merkt op dat het niet passend is om kritisch te zijn op de rol van de adoptieouder, gegeven het mandaat dat de adoptieouder heeft gekregen en gelet op de wijze waarop de Belastingdienst is georganiseerd. Zonder kaders en steun van boven is het moeilijk om Belastingdienst breed voortgang te boeken.

4.3 Sturing door directies zelf

De AP heeft gesprekken gevoerd met vertegenwoordigers van de directies MKB, P, GO en CAP. In de gesprekken werd ook de link gelegd met de ketens waarvoor de directeuren van die directies primair verantwoordelijk zijn.

Uit de gesprekken blijkt dat er vanuit directies diverse acties zijn ondernomen ten aanzien van LOA's. Zo hebben er bij verschillende directies inventarisaties plaatsgevonden om vast te stellen hoeveel LOA's er zijn, en in hoeverre LOA's bedrijfskritisch zijn. Die actie heeft er ook toe geleid dat er in 2024 diverse

¹⁵ AVG risico's bij inzet en gebruik LOA's, 18 juli 2024

¹⁶ Verslag gesprek AP/Belastingdienst, 6 maart 2025.



LOA's zijn omgezet in RTV's. De AP heeft vernomen dat dit in elk geval is gebeurd voor de LOA's die in gebruik zijn bij de directies P en MKB.

Ook vanuit CAP heeft een inventarisatie plaatsgevonden. 24 LOA's staan op de backlog om uitgefaseerd te worden. Niet duidelijk is wanneer de LOA's daadwerkelijk uitgefaseerd zijn. Dat is mede afhankelijk van de vraag wanneer de tekortkomingen in de legacy-systemen zijn opgelost.¹⁷

De datacoördinatoren zouden een cruciale rol kunnen spelen in het terugdringen van de LOA's, maar hun rol is beperkt. Datacoördinatoren worden over het algemeen marginaal betrokken bij het oplossen van de gap ten aanzien van de LOA's. Sommige datacoördinatoren hebben aangegeven een meer omvangrijke rol te willen vervullen in het terugdringen van LOA's, maar geven daarbij aan dat ze voor het succesvol vervullen van een dergelijke rol de daarvoor vereiste kaders vanuit de directie IV&D missen.¹⁸

4.4 Conclusie

Geconcludeerd wordt dat er geen centrale regie wordt gevoerd op de doelstelling om ketens en directies hun LOA's te laten voldoen aan de eisen welke voortvloeien uit wet- en regelgeving, waaronder de AVG en de BIO. De verantwoordelijkheid daarvoor is nagenoeg volledig bij de ketens en directies belegd. Vanuit ketens en directies zijn wel acties ondernomen om LOA's te inventariseren, en bedrijfskritische LOA's om te laten zetten in RTV's, maar deze acties hebben geen systematisch en gestructureerd karakter, gebaseerd op eenduidig Belastingdienst breed beleid. Er is geen zicht op de mate waarin deze acties succesvol zijn geweest.

Wel wordt er door middel van architectuurssturing vanuit IV&D een zekere mate van regie gevoerd op de doelstelling om het bestaan van bedrijfskritische LOA's terug te dringen. Deze regie heeft verdere versterking.

¹⁷ Voor veel van de legacy systemen zijn de tekortkomingen opgevangen met LOA's. Als de tekortkomingen zijn opgelost, zijn de LOA's niet meer nodig. Beantwoording vragen door CAP, naar aanleiding van het toezichtgesprek op 22 januari 2025.

¹⁸ Verslag gesprek AP/Belastingdienst met datacoördinator en business security officer MKB, 22 januari 2025.

5. LOA's en RTV's voor toezicht

5.1 Inleiding

In dit hoofdstuk worden de resultaten gepresenteerd van het onderzoek naar de LOA's en RTV's die persoonsgegevens verwerken en die in aanvulling daarop ook worden gebruikt voor toezichtdoeleinden.

De AP heeft de Belastingdienst verzocht om vragen te beantwoorden over LOA's en RTV's welke worden gebruikt voor toezichtdoeleinden. De in het onderzoek gestelde vragen zijn erop gericht om inzicht te verkrijgen in waar de applicaties voor dienen, welke persoonsgegevens de onderzochte applicaties verwerken, in hoeverre de risico's van die verwerkingen in kaart zijn gebracht, en in hoeverre deze verwerkingen voldoende beveiligd zijn.

De onderzochte applicaties dienen uiteenlopende doelen. Zo wordt bijvoorbeeld de LOA 'Grote Bouwprojecten Nederland' gebruikt om te controleren op juiste fiscale afdrachten bij grote bouwprojecten. Sommige LOA's of RTV's worden gebruikt om complexe of tijdrovende berekeningen welke binnen bepaalde processen dienen te worden gemaakt geautomatiseerd en daarmee sneller uit te voeren. Een voorbeeld hiervan is de applicatie 'CVP-module', waarmee voor bepaalde processen kan worden berekend wat de minimaal te verwachten loonheffing is die een werkgever moet afdragen. Andere applicaties worden gebruikt om bepaalde zaken te registreren. Zo wordt de RTV 'TV Vastgoed Fundament' gebruikt om signalen vast te leggen in het kader van transacties in onroerende zaken. Weer andere applicaties worden gebruikt om processen te faciliteren in het kader van bijzondere belastingmiddelen. Zo wordt de RTV 'Kansspelbelasting' onder meer gebruikt om aangiftes van bepaalde prijswinnaars van buitenlandse kansspelen te selecteren en vervolgens nader te controleren.

De resultaten van het onderzoek zijn gebaseerd op de ingevulde vragenlijsten voor 76 applicaties welke worden gebruikt voor het toezicht op Belastingplichting. Van deze applicaties zijn er 43 te classificeren als RTV's en 33 als LOA's.

De meeste LOA's zijn gebouwd met technologie die wordt aangeboden via de Microsoftproducten Microsoft Excel en Microsoft Access. 9 LOA's opereren op basis van Microsoft Excel, 21 LOA's opereren op basis van Microsoft Access.

Wanneer een LOA in beheer wordt genomen en daarmee een RTV wordt, is het over het algemeen de bedoeling dat deze applicaties door de Belastingdienst naar .NET applicaties worden omgeschreven. 14 RTV's opereren desalniettemin nog op basis van Microsoft Access. Voor 17 RTV's geldt dat hiervoor .NET geïmplementeerd. De rest van de RTV's opereren over het algemeen op UiPath, een software platform wat Robotic Process Automation (RPA) mogelijk maakt. Hiermee worden handmatige en repetitieve taken geautomatiseerd.

5.2 Persoonsgegevens en grondslag

Persoonsgegevens dienen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. Indien bijzondere persoonsgegevens worden verwerkt, waarbij de risico's voor de persoonlijke levenssfeer van betrokkenen groter zijn, zal ook dienen te worden aangetoond dat het verwerkingsverbod ten aanzien van bijzondere persoonsgegevens kan worden doorbroken.

Om na te gaan of de applicaties bestaande uit LOA's en RTV's welke worden gebruikt in het toezicht op belastingplichtigen voldoen aan het voornoemde grondslag- en doelbindingsvereiste, heeft de AP gevraagd welke categorieën persoonsgegevens de applicaties verwerken. Vervolgens is gevraagd of voor deze verwerkingen de grondslag is vastgesteld en of is vastgesteld of is voldaan aan het doelbindingsvereiste.

5.2.1 Welke persoonsgegevens

De AP heeft per applicatie welke wordt gebruikt in het toezicht op belastingplichtigen gevraagd welke categorieën persoonsgegevens er mee worden verwerkt. Voornamelijk daar waar gevoelige persoonsgegevens zoals het BSN, kenteken of adresgegevens worden verwerkt, bestaat het risico dat deze verwerkingen leiden tot een inbreuk op de rechten en vrijheden van burgers.

Van de 76 onderzochte applicaties worden er in 37 applicaties adresgegevens verwerkt waarbij het onder meer gaat om adresgegevens van belastingplichtigen. In 53 applicaties wordt het BSN verwerkt. Daarnaast verwerken 6 applicaties het kenteken van belastingplichtigen.

Ten aanzien van de onderzochte applicaties is ook gevraagd of deze bijzondere persoonsgegevens verwerken. Daarvan is door de Belastingdienst aangegeven dat in principe geen enkele applicatie bijzondere persoonsgegevens verwerkt. De Belastingdienst zal echter rekening moeten houden met de mogelijkheid dat persoonsgegevens, gelet op een mogelijke combinatie met andere persoonsgegevens, maar ook gelet op de context van de verwerking, in bepaalde gevallen kunnen worden geclassificeerd als bijzondere persoonsgegevens. Een voorbeeld hiervan is het afkunnen leiden van iemands seksuele gerichtheid uit diens burgerlijke staat en de combinatie daarvan met andere gegevens.

De Belastingdienst zal alert moeten blijven op de mogelijke verwerking van bijzondere persoonsgegevens. Zeker waar deze gegevens worden verwerkt binnen LOA's en RTV's is het nagaan of mogelijk bijzondere persoonsgegevens kunnen worden afgeleid van belang, omdat deze applicaties doorgaans niet voldoende beveiligd zijn, terwijl voor bijzondere persoonsgegevens juist aanvullende bescherming noodzakelijk is.

5.2.2 Grondslag

Elke verwerking van persoonsgegevens dient gebaseerd te zijn op een van de grondslagen uit de AVG. De AP heeft per applicatie gevraagd of de grondslag voor de verwerkingen welke worden uitgevoerd met die applicatie aantoonbaar is vastgesteld.



Van de 76 onderzochte applicaties is er voor 7 applicaties niet vastgesteld wat de grondslag is voor de in die applicatie verwerkte persoonsgegevens. Dit betroffen allemaal LOA's.

Om rechtszekerheid voor betrokkenen en de voorspelbaarheid van de verwerking van persoonsgegevens van deze betrokkenen te waarborgen dient vóórdat enige verwerking van persoonsgegevens plaatsvindt te zijn bepaald op basis van welke grondslag deze verwerking kan plaatsvinden. Het voorafgaand aan de verwerking vaststellen van de grondslag van de verwerking is dan ook een van de kernbeginselen uit de AVG.

De AP concludeert dat de Belastingdienst niet voldoet aan het vereiste om voor alle verwerkingen van persoonsgegevens aantoonbaar te maken dat deze berusten op de hiervoor noodzakelijke grondslag. De AP ziet het dan ook als zorgelijk dat de Belastingdienst niet voldoet aan de aantoonplicht uit de AVG.

5.2.3 Doelbinding

Persoonsgegevens mogen niet verder worden verwerkt op een wijze welke onverenigbaar is met de oorspronkelijke doeleinden van de verwerking. Niet voldoen aan het doelbindingsvereiste kan er onder meer toe leiden dat gevoelige informatie in een verkeerde context terechtkomt en dat daarbij gegevens over een persoon mogelijk onjuist worden geïnterpreteerd, hetgeen kan leiden tot nadelige gevolgen voor de betrokkene. Het doelbindingsvereiste zorgt ervoor dat betrokkenen weten voor welke doeleinden hun persoonsgegevens worden verwerkt en versterkt de controle welke betrokkenen over hun persoonsgegevens uit kunnen oefenen. Daarom is het van groot belang om vast te stellen of er met de verwerking van persoonsgegevens wordt voldaan aan het doelbindingsvereiste.

Het gebruik van LOA's vergroot de kans dat er niet wordt voldaan aan het doelbindingsvereiste. LOA's zijn afhankelijk van (persoons)gegevens welke worden onttrokken uit reguliere IV-applicaties. Verwerkingen van persoonsgegevens welke voortkomen uit het gebruik van LOA's zijn dan ook te classificeren als verdere verwerkingen waarvoor dient te worden vastgesteld of deze nog verenigbaar zijn met de oorspronkelijke doeleinden van de verwerking.

De AP heeft per applicatie gevraagd of er voor de verwerkingen welke worden uitgevoerd met de applicatie is vastgesteld of wordt voldaan aan het vereiste van doelbinding.

Van de 76 onderzochte applicaties is er voor 13 applicaties niet duidelijk of is vastgesteld of de verwerkingen van persoonsgegevens in die applicatie voldoen aan het doelbindingsvereiste. Een groot aantal van de applicaties waarvoor dit niet inzichtelijk is vallen onder de verantwoordelijkheid van de directie MKB.

Een voorbeeld van een applicatie waarvan niet duidelijk is of er voldaan is aan het doelbindingsvereiste is de RTV genaamd 'PLH' welke in het kader van loonheffing wordt gebruikt door toezichtmedewerkers om signalen af te handelen. Een andere applicatie waarvoor dit geldt is de LOA 'PGA Workflow' welke onder meer wordt gebruikt om risicosignalen te behandelen in het kader van het aangegeven uitsluitend zakelijk gebruik van bestelauto's.

De AP stelt vast dat de Belastingdienst niet aantoonbaar heeft gemaakt dat de verwerkingen van persoonsgegevens in deze applicaties voldoen aan het doelbindingsvereiste en daarmee rechtmatig zijn.

5.2.4 Exportfunctie

Wanneer een applicatie de mogelijkheid biedt om persoonsgegevens te exporteren kan dit leiden tot de situatie dat er geen zicht meer is op wie toegang heeft tot deze gegevens, of deze gegevens rechtmatig worden gedeeld en of deze gegevens nog voldoende worden beveiligd. Omdat LOA's buiten de domeinarchitectuur van de Belastingdienst opereren wordt het risico om dit zicht te verliezen bij dit soort applicaties met een exportfunctie aanzienlijk groter.

De functionaliteit van veel LOA's en RTV's is het filteren, verifiëren, combineren of verrijken van gegevens uit een of meer systemen van de Belastingdienst. De informatiestromen uit deze bronsystemen waren voor de ontwikkelaars van deze applicaties vrij toegankelijk. Mede door die toegankelijkheid werd het digitale 'ecosysteem' gefaciliteerd waarin deze applicaties gebouwd konden worden.

De Belastingdienst probeert grip op de export te krijgen door gegevens(stromen) alleen op basis van aangetoonde noodzakelijkheid vrij te geven via een data-loket. De hoop van de Belastingdienst is dat door het afknijpen van de mogelijke invoer van gegevens in de schaduw-ICT, de mogelijkheid tot het maken van nieuwe LOA's teniet wordt gedaan.

Bij de bestaande LOA's met een exportfunctie bestaat het risico dat deze ook zonder instroom van nieuwe gegevens uit geverifieerde systemen een systeem van verwerkingen in stand houden. Dit omdat deze LOA's nog kunnen opereren op basis van de informatie welke daarin reeds is opgeslagen. Daarbij ontstaat een risico van verwerkingen op basis van verouderde en niet geverifieerde informatie, en het risico op het ontstaan van nieuwe LOA's uit de informatiestromen uit de reeds bestaande LOA's.

De AP heeft per applicatie gevraagd of deze de mogelijkheid bezit om gegevens uit de omgeving van de applicatie te exporteren. Van de 76 onderzochte applicaties hebben er 49 een exportfunctie. Dat is een zorgelijk hoog aantal.

5.2.5 Verstrekking aan andere organisaties

De AP heeft gevraagd bij hoeveel van deze applicaties de gegevens worden doorgestuurd naar andere organisaties. Van de 49 applicaties met een exportfunctie worden er van 8 applicaties ook gegevens doorgestuurd naar andere organisaties. Een voorbeeld van een applicatie waarbij gegevens worden verstrekt aan andere organisaties is de LOA 'BRE' welke wordt gebruikt in het kader van de omzetbelasting op e-commerce binnen de EU. Met deze applicatie wordt statistische informatie doorgestuurd naar het CBS.

Daarnaast worden er gegevens verstrekt aan andere organisaties vanuit de applicatie Informatiesjabloon. Deze applicatie wordt gebruikt in het toezicht om gegevens van belastingplichtigen uit diverse reguliere IV-applicaties te combineren en overzichtelijk weer te geven. Sommige overzichten die met deze LOA worden gemaakt kunnen naar aanleiding van een vordering om gegevens in het kader van een strafrechtelijk onderzoek worden toegestuurd aan het OM en Politie. Daarnaast worden sommige van deze in Informatiesjabloon gemaakte overzichten doorgezonden aan de Kansspelautoriteit en het Landelijk Bureau Bibob in het kader van toezicht op misbruik van vergunningen en subsidies. De AP heeft bij brief

van 9 juli 2025 aan de Staatssecretaris van Fiscaliteit, Belastingdienst en Douane verzocht om de applicatie Informatiesjabloon op de kortst mogelijke termijn uit te faseren.¹⁹

De AP concludeert dat de Belastingdienst door het gebruik van LOA's onvoldoende zicht heeft op welke persoonsgegevens worden verstrekt aan andere organisaties en of deze verstrekkingen in alle gevallen rechtmatig zijn.

5.2.6 Bewaren van gegevens

Persoonsgegevens dienen niet langer te worden bewaard dan voor de doeleinden van de verwerking noodzakelijk is. Teneinde te voldoen aan dit aspect van het beginsel van opslagbeperking dient een verwerkingsverantwoordelijke een bewaartermijn voor persoonsgegevens vast te stellen.

Door persoonsgegevens niet langer te bewaren dan noodzakelijk wordt het risico dat deze gegevens op een onrechtmatige wijze worden verwerkt beperkt. Daarnaast verkleint het de kans dat er ten opzichte van deze persoonsgegevens een inbreuk plaatsvindt.

De AP heeft per applicatie gevraagd of voor de persoonsgegevens welke worden verwerkt in de applicatie een bewaartermijn is vastgesteld. Vervolgens is de vraag gesteld of deze persoonsgegevens dan ook conform deze vastgestelde bewaartermijn worden verwijderd of gearchiveerd.

Van de 76 onderzochte applicaties is er voor 9 applicaties geen bewaartermijn vastgesteld voor de persoonsgegevens welke daarin worden verwerkt. Van 3 applicaties is aangegeven dat niet bekend is of er een vastgestelde bewaartermijn is.

Voor de applicaties waarvoor de bewaartermijn wel is vastgesteld worden bij 3 applicaties de persoonsgegevens niet conform deze bewaartermijn verwijderd of gearchiveerd. Bij 1 applicatie is niet bekend of persoonsgegevens worden verwijderd of gearchiveerd conform de bewaartermijn.

De AP concludeert dat de vereiste bewaartermijnen voor persoonsgegevens welke worden verwerkt in de onderzochte applicaties niet altijd zijn vastgesteld. Daarnaast ziet de AP dat indien deze bewaartermijn wel is vastgesteld, dit nog niet betekent dat deze gegevens ook daadwerkelijk conform deze bewaartermijn worden verwijderd of gearchiveerd.

5.3 Risicoanalyses

Zowel het gebruik van LOA's als RTV's kan gepaard gaan met risico's. Enerzijds betreffen dit risico's voor de persoonlijke levenssfeer van betrokkenen. Anderzijds betreffen dit risico's voor de bedrijfscontinuïteit, welke vervolgens negatieve gevolgen kunnen hebben voor de dienstverlening richting burgers. Teneinde deze risico's inzichtelijk te maken en te adresseren is het noodzakelijk om een risicoanalyse uit te voeren.

¹⁹ Gelet op de risico's welke het gebruik van deze applicatie met zich meebrengt voor de rechten en vrijheden van belastingplichtigen heeft de AP de Belastingdienst opgedragen om een plan te maken om de applicatie Informatiesjabloon te vervangen. Daarnaast heeft de AP de Belastingdienst ook opgedragen om in de tussentijd mitigerende maatregelen te treffen om de risico's van het gebruik te beperken.

5.3.1 Risicoanalyses voor betrokkenen

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dient de verwerkingsverantwoordelijke een beoordeling uit te voeren van het effect van de verwerkingsactiviteit op de bescherming van persoonsgegevens (gegevensbeschermingseffectbeoordeling of GEB).

Door middel van het uitvoeren van een GEB op de verwerkingen van persoonsgegevens welke worden gefaciliteerd door een applicatie worden de risico's welke gepaard gaan met die verwerkingen inzichtelijk. Dit stelt de verwerkingsverantwoordelijke in staat om deze risico's te adresseren, teneinde de persoonlijke levenssfeer van de natuurlijke personen wiens gegevens worden verwerkt te beschermen. Bij het uitblijven van een dergelijke risicoanalyse blijven risico's voor betrokkenen mogelijk ongeadresseerd, waardoor de kans op inbreuken op de persoonlijke levenssfeer groot is.

De Belastingdienst hanteert twee instrumenten voor het in kaart brengen van de risico's voor betrokkenen welke gepaard gaan met een verwerking van persoonsgegevens. Enerzijds wordt de door de AVG voorgeschreven gegevensbeschermingseffectbeoordeling (GEB) hiervoor gebruikt. Daarnaast wordt echter ook een zogenaamde Privacy Risico Analyse (PRA) gebruikt als middel om deze risico's in kaart te brengen.

Een PRA kan worden gezien als een lichtere vorm van een GEB, welke sneller kan worden uitgevoerd maar wel een systematische analyse van risico's voor de persoonlijke levenssfeer van betrokkenen behelst. De AP merkt op dat een PRA niet voldoet aan de wettelijke vereisten welke de AVG voor een GEB voorschrijft. Het uitvoeren van een PRA vrijwaart de Belastingdienst derhalve ook niet van de verplichting om, indien de noodzaak daartoe volgt uit artikel 35 AVG, een GEB uit te voeren.

Uiteraard kan een dergelijke PRA wel dienen als een instrument om op een laagdrempelige wijze al risico's voor de persoonlijke levenssfeer van betrokkenen te identificeren en zo nodig te mitigeren.

De AP heeft per applicatie gevraagd of voor de persoonsgegevens welke worden verwerkt in de applicatie een systematische beoordeling van de risico's van die verwerking heeft plaatsgevonden. Naast het hebben uitgevoerd van een GEB valt hier ook het hebben uitgevoerd van een PRA onder.

Vervolgens heeft de AP gevraagd of er in het uitvoeren van die systematische risicoanalyse hoge risico's voor de persoonlijke levenssfeer van betrokkenen zijn geïdentificeerd, en of het gelukt is om deze hoge risico's te mitigeren tot een acceptabel niveau.

Van de 76 onderzochte applicaties is er voor de processen welke gebruik maken van deze applicaties slechts 8 keer een GEB of PRA uitgevoerd. Van 2 van deze 8 applicaties wordt aangegeven dat er met het uitvoeren van de risicoanalyse hoge risico's zijn geconstateerd. Van deze hoge risico's wordt aangegeven dat deze zijn gemitigeerd tot een acceptabel niveau. Voor 11 van de 76 onderzochte applicaties is aangegeven dat het niet bekend is of er een systematische risicoanalyse is uitgevoerd. In de overige 57 gevallen is geen analyse uitgevoerd.

De AP concludeert dat de Belastingdienst voor het overgrote deel van de onderzochte applicaties niet op een systematische wijze in kaart heeft gebracht welke risico's de verwerkingen welke daarmee worden uitgevoerd hebben voor de persoonlijke levenssfeer van betrokkenen.

Omdat de onderzochte applicaties zijn ontwikkeld buiten de kaders van de reguliere IV van de Belastingdienst, is de kans groot dat ze gebreken vertonen in privacybeschermende en informatiebeveiligingsmaatregelen. Dat maakt dat juist voor deze applicaties op systematische wijze in kaart dient te worden gebracht welke risico's het gebruik ervan mogelijk teweegbrengt voor de persoonlijke levenssfeer van burgers wiens persoonsgegevens met de applicatie worden verwerkt. De afwezigheid van systematische risicoanalyses ten opzichte van deze applicaties ziet de AP dan ook als zorgwekkend.

5.3.2 Risicoanalyses bedrijfscontinuïteit

Het gebruik van LOA's en RTV's kan ook risico's met zich meebrengen voor de bedrijfscontinuïteit. Voor LOA's zijn geen algemene maatregelen geïmplementeerd om een vastgesteld niveau van beschikbaarheid te waarborgen.²⁰ Voor RTV's welke zijn gebouwd op zogenaamde 'end-of-life technology' zoals Microsoft Excel of Microsoft Access wordt door het deze applicaties beherende LIV aangegeven dat deze eveneens risico's met zich meebrengen voor de bedrijfscontinuïteit. Dit vergroot het risico op het uitvallen van deze applicaties, en daarmee voor de continuïteit van de processen van de Belastingdienst.

De AP heeft per applicatie gevraagd of de risico's van het gebruik van de applicatie in het kader van bedrijfscontinuïteit op een systematische wijze in kaart zijn gebracht.

Vervolgens heeft de AP gevraagd of er in het uitvoeren van die systematische risicoanalyse hoge risico's voor de bedrijfscontinuïteit zijn geïdentificeerd, en of het gelukt is om deze hoge risico's te mitigeren tot een acceptabel niveau.

Van de 76 onderzochte applicaties is er voor 32 applicaties een analyse uitgevoerd naar de risico's in het kader van bedrijfscontinuïteit. Bij 17 van deze applicaties is vastgesteld dat er met het gebruik van de applicatie een hoog risico bestaat voor de bedrijfscontinuïteit. Het merendeel hiervan betreffen LOA's welke onder het beheer zijn van de directie MKB en waarvoor de keten Omzetbelasting verantwoordelijk is. Een voorbeeld van een applicatie waarvoor hoge risico's zijn geïdentificeerd is de LOA 'Topboetes' welke wordt gebruikt voor het beoordelen en bijstellen van op te leggen verzuimboetes bij het MKB.

Van één applicatie wordt aangegeven dat niet gelukt is om het hoge risico te mitigeren tot een acceptabel niveau. Dit betreft een RTV bestaande uit een script welke het mogelijk maakt om aangiftes in het kader van grensarbeid deels geautomatiseerd af te handelen. De AP roept de Belastingdienst dringend op om na te gaan of deze applicatie niet beter buiten werking kan worden gesteld of met spoed om te bouwen tot een reguliere applicatie.

De AP ziet dat er voor een significant aantal applicaties geen risicoanalyse in het kader van de bedrijfscontinuïteit is uitgevoerd. Voor de applicaties waarbij een dergelijke risicoanalyse wél is uitgevoerd geldt dat dit in meer dan de helft van de gevallen heeft geleid tot de identificatie van hoge risico's.

5.4 Beveiliging

²⁰ Dit volgt uit het memo 'AVG richtlijnen bij de inzet van een LOA' 8-1-2025.



De Belastingdienst moet passende technische en organisatorische maatregelen treffen om de verwerkingen van persoonsgegevens te beschermen. Die verantwoordelijkheid geldt onverminderd voor LOA's en RTV's.

In het onderzoek naar de LOA's en RTV's welke worden gebruikt voor toezicht zijn een aantal vragen gesteld om na te gaan welke beveiligingsmaatregelen bij deze applicaties zijn toegepast om een passend beveiligingsniveau te waarborgen. Er is gevraagd in hoeverre maatregelen in het kader van autorisatiebeheer, registratie van gebeurtenissen, het maken van back-ups en versleuteling zijn toegepast. Op basis hiervan toetsen we in hoeverre beveiligingsmaatregelen die afgeleid kunnen worden uit de Baseline Informatiebeveiliging Overheid (BIO) of de Basisprincipes van Digitale Weerbaarheid van het NCSC en het DTC²¹ om een passend beveiligingsniveau te waarborgen, zijn toegepast bij LOA's en RTV's.

5.4.1 Autorisatiebeheer

Autorisatiebeheer is de wijze waarop wordt voorzien in het regelen van toegang tot informatie en systemen. Autorisatiebeheer moet voorkomen dat gebruikers toegang hebben tot systemen of tot informatie welke zij uit hoofde van hun werkzaamheden niet nodig hebben. Een systeem voor autorisatiebeheer beschermt daarmee de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens. In autorisatiebeheer ligt niet alleen nadruk op het voorkomen van toegang tot systemen of informatie door actoren van buiten de organisatie. Het moet er ook voor zorgen dat interne gebruikers in de organisatie alleen toegang krijgen tot informatie welke passend is bij hun rol en bij de taken die zij dienen uit te voeren.

In het geval van LOA's of RTV's is er een verhoogd risico dat informatie toegankelijk wordt gemaakt aan gebruikers die daar volgens het reguliere autorisatiebeleid geen toegang toe zouden moeten hebben. Dat kan onder andere leiden tot een inbreuk op de vertrouwelijkheid van informatie, maar kan bijvoorbeeld ook leiden tot het nemen van besluiten over belastingplichtigen op basis van niet gevalideerde gegevens.

Een autorisatieconcept is een model om toegangsrechten te structureren en beheren. De Belastingdienst hanteert Role-Based Access Control (RBAC) als autorisatieconcept. Met dit autorisatieconcept worden rechten toebedeeld aan vooraf gedefinieerde rollen. Gebruikers krijgen vervolgens een of meer van deze rollen toebedeeld, en daarmee ook de daaraan gekoppelde autorisaties. Het systeem dat de Belastingdienst gebruikt om dit autorisatieconcept toe te passen en te beheren is het Identity Management System (IMS). Dit is een technische voorziening waarmee de identiteiten van gebruikers kunnen worden beheerd en waarmee rollen en rechten kunnen worden toegekend aan gebruikers. Het IMS dient te waarborgen dat autorisaties geautomatiseerd, gecontroleerd en consistent worden toegepast binnen de organisatie.

Een autorisatiematrix, of een rechtenmatrix is een documentatie-instrument waarmee op een systematische manier wordt beschreven welke autorisaties moeten worden toegekend aan welke gebruikers. Zo kan er in een autorisatiematrix worden uitgewerkt welke rollen er in een applicatie bestaan en welke rechten elke rol heeft. Deze organisatorische maatregel geeft daarmee inzicht in wie toegang heeft tot gegevens in een applicatie, en toont vervolgens ook aan dat deze toegang noodzakelijk en proportioneel is.

²¹ <https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes>.

In de referentiearchitectuur van de Belastingdienst wordt de noodzaak tot het beperken van niet noodzakelijk toegang onderschreven aan de hand van het *'need-to-know'* principe.²² Dit principe houdt onder meer in dat een gebruiker of beheerder alleen inzage heeft in die gegevens die noodzakelijk zijn voor het uitvoeren van toegekend werk. Omdat RTV's worden opgenomen in de architectuur van de Belastingdienst, is te verwachten dat voor deze applicaties de voorwaarden voor toegang tot gegevens expliciet zijn vastgelegd.

De Belastingdienst heeft aangegeven bij 43 van de 76 applicaties een autorisatiematrix opgesteld te hebben. Bij 66 van de 76 applicaties is er een vorm van Role-Based Access Control (RBAC) van toepassing op de applicatie, waarvan het in 57 gevallen zag op toepassing van RBAC doormiddel van het generieke IMS van de Belastingdienst.

Van alle RTV's wordt aangegeven dat er gebruikt wordt gemaakt van het IMS, maar bij slechts 24 van de 43 applicaties wordt expliciet aangegeven dat daar een autorisatiematrix voor is opgesteld.

Dit is zorgelijk omdat met een autorisatiematrix aantoonbaar wordt gemaakt dat de toegang tot gegevens binnen een applicatie noodzakelijk en proportioneel is. Daarnaast maakt de afwezigheid van een autorisatiematrix dat het niet inzichtelijk is welke gebruiker welke rechten heeft en wat de gevolgen daarvan zijn. Dit kan er onder andere toe leiden dat gebruikers rechten verwerven welke misbruik of fraude mogelijk maken. Een voorbeeld hiervan is de autorisatie om een betaling te doen en de autorisatie om deze betaling goed te keuren.

In 19 van de 43 RTV's zijn de voorwaarden waaraan een gebruiker moet voldoen om toegang te krijgen tot de applicatie of gegevens in de applicatie niet vastgelegd. Een voorbeeld van een dergelijke applicatie is STER, een enquêtetool voor het vastleggen van de antwoorden van de behandelaar ten behoeve het steekproevenonderzoek bij erfbelasting. Dit is opmerkelijk omdat RTV's vallen onder de architectuur van de Belastingdienst, waarin het de bedoeling is dat het hiervoor benoemde *'need-to-know'* principe wordt toegepast.

Ondanks dat ongecontroleerde toegang tot gegevens bij LOA's niet minder kwalijk is, ligt het in de lijn der verwachting dat de voorwaarden om toegang te krijgen tot LOA's en de gegevens daarin niet zijn vastgelegd. LOA's maken immers geen onderdeel uit van de architectuur van de Belastingdienst. Het is dan ook opmerkelijk dat bij 12 van de 33 LOA's de voorwaarden om toegang te krijgen wél zijn vastgelegd.

De AP concludeert dat de maatregelen rondom toegangsbeheer voor LOA's en RTV's door de Belastingdienst onvoldoende gedocumenteerd en geïmplementeerd zijn. De AP ziet dat voor bijna de helft van de RTV's nog geen autorisatiematrix is opgesteld, en dat ook de voorwaarden voor toegang niet zijn vastgesteld. De AP merkt op dat de Belastingdienst onvoldoende grip heeft op het autorisatiebeheer ten aanzien van RTV's.

5.4.2 Loggen en monitoren van de gebruikersactiviteiten

Het vastleggen en monitoren van de gebruikersactiviteiten (logging en monitoring) is een belangrijke maatregel om het risico op onbevoegd en onbedoeld gebruik van gegevens en systemen te mitigeren. Deze maatregel werkt vaak aanvullend en controlerend op een toegepast systeem van autorisaties en is onmisbaar wanneer het autorisatiebeheer gebreken vertoont. Met het loggen en monitoren van

²² Referentiearchitectuur Integrale Beveiliging (Editie: Q1 2020)



gebruikersactiviteiten is het mogelijk om onrechtmatige toegang tot gegevens te detecteren en hierop te handelen. Ook biedt logging de mogelijkheid om na afloop van een incident te analyseren wat er zich exact heeft afgespeeld. Het daadwerkelijk monitoren van deze logbestanden vormt dan ook een onmisbaar onderdeel om het risico op onrechtmatige toegang tot gegevens te mitigeren.

In aanvulling op deze detecterende werking van logging en monitoring kan deze maatregel ook een preventieve werking hebben. Wanneer gebruikers weten dat hun handelingen worden vastgelegd en worden gecontroleerd op mogelijk onrechtmatige handelingen, voorkomt dit dat gebruikers gegevens benaderen welke zij uit hoofde van hun werkzaamheden niet hoeven te benaderen.

Voor het onderzoek naar LOA's en RTV's welke worden gebruikt in het toezicht is de Belastingdienst gevraagd voor welke van de applicaties de activiteiten van gebruikers van de applicatie worden geregistreerd (logging). Voor 41 van de 76 applicaties wordt aangegeven dat er een vorm van logging plaatsvindt. Daarvan waren er 21 LOA's en 20 RTV's.

Bij slechts 4 van deze applicaties is aangegeven dat de gemaakte logbestanden regelmatig worden gecontroleerd. Dit betroffen allemaal LOA's.

Hieruit blijkt dat logging en monitoring van gebruikersactiviteiten als maatregel slechts in 4 van de 76 onderzochte applicaties als beveiligingsmaatregel wordt toegepast.

Hoewel het vastleggen en monitoren van gebeurtenissen onder andere op basis van de BIO een verplichte maatregel is, kan deze verplichting in bepaalde gevallen vervallen. Het uitvoeren van een risicoanalyse welke rekening houdt met de risico's voor betrokken zal dan vereist zijn om te bepalen of het loggen en monitoren van gebruikersactiviteiten mogelijk anderszins niet noodzakelijk is.

Van de 23 RTV's waar geen logging bij plaatsvindt is slechts in 3 gevallen een risicoanalyse uitgevoerd.

De AP concludeert dat de Belastingdienst in minder dan de helft van de RTV's aan logging doet. Geen van deze logging bij RTV's wordt gemonitord. Het baart de AP grote zorgen dat de beveiligingsmaatregelen van logging en controle op de logging nagenoeg afwezig zijn.

5.4.3 Maken van een back-up van de applicatie

Ter bescherming tegen verlies van gegevens, voor het behoud van de bedrijfscontinuïteit en om de totstandkoming van geautomatiseerde beslissingen herleidbaar te houden, is het belangrijk om een back-up beleid te hebben. Regelmatig behoren back-upkopieën van informatie, software en systeemaftbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.²³

In 70 van de 76 applicaties geeft de Belastingdienst aan dat er een back-up wordt gemaakt van de applicatie.

De AP concludeert dat de medewerkers van de Belastingdienst – zelfs voor de schaduw-ICT waar de afdeling IV geen regie op heeft – meestal mechanismen in gebruik hebben om back-ups te maken van deze applicaties. Dat is positief.

²³ BIO v1.0.4zv 12.3.1

6. Conclusies en noodzakelijke maatregelen

6.1 Inleiding

In dit hoofdstuk worden de belangrijkste conclusies van het onderzoek naar het bestaan en gebruik van LOA's en RTV's binnen de Belastingdienst samengevat.

Op basis van de conclusies en bevindingen uit dit rapport komt de AP met noodzakelijke maatregelen om de risico's voor de bescherming van de persoonlijke levenssfeer van burgers welke voortkomen uit het bestaan en gebruik van schaduw-ICT te mitigeren.

6.2 Samenvatting conclusies

6.2.1 Beleid, inzicht en regie

De Belastingdienst beschikt niet over een accuraat centraal overzicht van LOA's. Er is bij IV&D wel enig zicht op de bedrijfskritische LOA's, maar de administratie daaromtrent behoeft nog verbetering. Omdat dit betrouwbare inzicht ontbreekt kan ook niet worden vastgesteld hoe het aantal LOA's zich ontwikkelt.

De Belastingdienst heeft geen centraal beleid ten aanzien van het gebruik van LOA's en RTV's in het licht van de eisen welke voortvloeien uit wet- en regelgeving, waaronder de AVG en de BIO. Er is geen centraal vastgesteld beleid aangetroffen waaruit blijkt aan welke eisen LOA's en RTV's moeten voldoen voor de periode dat deze applicaties nog niet zijn omgezet in reguliere applicaties binnen de domeinarchitectuur. De Belastingdienst weet daardoor niet in hoeverre de nog in gebruik zijnde LOA's en RTV's voldoen aan de eisen op het gebied van privacy en informatiebeveiliging.

De verantwoordelijkheid voor het laten voldoen van LOA's en RTV's aan de hierboven genoemde kaders is nagenoeg volledig bij de ketens en directies belegd. Er is geen zicht op de mate waarin LOA's en RTV's aan de kaders voldoen.

Vanuit ketens en directies zijn wel acties ondernomen om LOA's te inventariseren, en bedrijfskritische LOA's om te laten zetten in RTV's, maar deze acties hebben geen systematisch en gestructureerd karakter, gebaseerd op eenduidig Belastingdienst breed beleid. Er is geen zicht op de mate waarin deze acties succesvol zijn geweest.

Door middel van architectuurssturing wordt wel een zekere mate van regie gevoerd op de doelstelling om het bestaan van bedrijfskritische LOA's terug te dringen. Voor zover deze applicaties niet voldoen aan de daarin gestelde kaders, dient bij opname in de architectuurrepository door de domeinarchitecten te worden aangegeven wanneer deze afwijkingen ten opzichte van de kaders worden opgelost door middel van zogenaamde werkpakketten.

6.2.2 LOA's en RTV's voor toezicht

De AP heeft onderzoek gedaan naar 76 applicaties welke getypeerd worden als een LOA of een RTV en welke worden gebruikt voor het toezicht op belastingplichtigen.



Uit dit onderzoek bleek dat niet voor alle verwerkingen welke binnen deze applicaties plaatsvonden de grondslag of doelbinding was vastgesteld. Voor de grondslag was dit niet vastgesteld bij 7 van de 76 applicaties. De vereiste doelbinding was bij 13 van de 76 applicaties niet vastgesteld. Dit is ernstig omdat het vaststellen hiervan essentieel is om rechtszekerheid voor betrokkenen en de voorspelbaarheid van de verwerking van persoonsgegevens van deze betrokkenen te waarborgen.

Veel van de onderzochte applicaties hebben een exportfunctie. De Belastingdienst heeft onvoldoende zicht op de vraag welke gegevens mogelijk buiten de beveiligde omgeving van de organisatie terechtkomen. Van de 76 applicaties hebben er maar liefst 49 een exportfunctie.

Tevens bleek dat voor de meeste applicaties geen risicoanalyses waren uitgevoerd. Zowel ten aanzien van de risico's voor belastingplichtigen, als ten aanzien van risico's voor de bedrijfsvoering bleek dat er nagenoeg geen systematische analyses waren uitgevoerd om mogelijke risico's in kaart te brengen en zo nodig te mitigeren.

Tot slot bleek ook dat het autorisatiebeheer van deze applicaties niet in alle gevallen voldeed aan de daarvoor gestelde eisen. Logging en monitoring van gebruikersactiviteiten, een beveiligingsmaatregel welke de risico's van een gebrekkig autorisatiebeheer kunnen adresseren, bleek ook nagenoeg niet te zijn geïmplementeerd.

6.3 Overkoepelende conclusies

De AP concludeert dat er onvoldoende gestuurd wordt op het laten voldoen van LOA's en RTV's, en de verwerkingen van persoonsgegevens daarin, aan de eisen van wet- en regelgeving op het punt van de bescherming van persoonsgegevens. Er is te weinig inzicht, het ontbreekt aan eenduidig richtinggevend beleid, en aan toereikende centrale regie. Burgers lopen daardoor het risico dat er onzorgvuldig met hun persoonsgegevens wordt omgegaan, bijvoorbeeld doordat gegevens langer worden bewaard dan nodig, niet voldoende worden beveiligd, dat verouderde gegevens niet worden verwijderd of zelfs dat op basis van verouderde gegevens verkeerde beslissingen worden genomen.

De verantwoordelijkheid om tot minder LOA's te komen ligt voor het grootste deel bij de ketens en directies. Door de verantwoordelijkheid in overwegende mate bij de ketens en directies te beleggen, en deze verantwoordelijkheid onvoldoende te ondersteunen met een *duidelijke* kaderstelling vanuit de directie Informatievoorziening & databeheersing (IV&D) en een sterk gevoerde regie op de uitvoering van deze kaders, blijft de aanpak van LOA's diffuus, onoverzichtelijk en niet doelmatig. Dit terwijl juist het bestaan van LOA's binnen de verschillende ketens is aangemerkt als een generiek probleem waarvoor een generieke aanpak voor de gehele Belastingdienst zou moeten worden ontwikkeld.

In juli 2024 is het thema LOA's door de Belastingdienst aangemerkt als een 'gap'. Helaas heeft dit niet geleid tot een adequate aanpak om dit probleem aan te pakken. De acties die in 2024 zijn ondernomen zijn voor een groot deel verzand en gestrand.

6.4 Noodzakelijke maatregelen

6.4.1 Noodzakelijke maatregelen ten aanzien van LOA's en RTV's

Gelet op de risico's welke het gebruik van LOA's en RTV's met zich mee kunnen brengen voor de rechten en vrijheden van belastingplichtigen, dient de Belastingdienst controle te krijgen op het bestaan en gebruik van deze applicaties. Gelet op de conclusies van dit rapport ziet de AP de noodzaak tot het treffen van de volgende maatregelen:

1. Toets in hoeverre vigerende LOA's en RTV's voldoen aan de AVG en de BIO en voer daar waar vereist risicoanalyses uit voor de verwerkingen welke worden uitgevoerd met deze applicaties.
2. Versterk de regie vanuit de directie IV&D. Draag daarbij zorg voor concrete kaders ten aanzien van het bestaan en gebruik van LOA's en RTV's. Zorg voor een centraal overzicht van (bedrijfskritische) LOA's op basis waarvan kan worden gestuurd op de doelstelling om het bestaan van deze applicaties terug te dringen.
3. Stel een plan op waaruit blijkt hoe en binnen welke termijn LOA's en RTV's moeten worden omgezet in reguliere applicaties, en voer dat plan vervolgens uit. Werk daarin ook uit in welke situaties een LOA of RTV moet worden stopgezet.
4. Beperk de mogelijkheden tot gegevensleveringen uit bestaande bronssystemen aan LOA's zodat het ontstaan van (bedrijfskritische) LOA's wordt teruggedrongen. Zorg ervoor dat nieuwe (bedrijfskritische) LOA's uitsluitend ontstaan als dit volgens een lid van het bestuursteam dringend noodzakelijk is bevonden en mits deze voldoen aan daaraan te stellen eisen.

6.4.2 Toets LOA's en RTV's aan de AVG en de BIO en voer daar waar vereist risicoanalyses uit

Doordat de Belastingdienst LOA's en RTV's voor bepaalde primaire processen onmisbaar heeft laten worden, kan het uitzetten van deze applicaties grote gevolgen hebben voor de diensten welke de Belastingdienst dagelijks levert aan burgers. Anderzijds dienen ook deze applicaties te voldoen aan de eisen uit de AVG en de BIO. Nagaan of het gebruik van deze applicaties voldoet aan de AVG en de BIO is des te meer van belang nu deze zijn voortgebracht buiten de vastgestelde kaders van de Belastingdienst op het gebied van privacy en informatiebeveiliging.

Essentieel onderdeel en het startpunt van een dergelijke toetsing is het vaststellen van de grondslag en de vereiste doelbinding voor deze verwerkingen. Dit is cruciaal om de rechtszekerheid voor betrokkenen en de voorspelbaarheid van de verwerking van persoonsgegevens van deze betrokkenen te waarborgen.

Zorg dat voor alle gegevensverwerkingen in de LOA's is vastgesteld wat de grondslag is voor de verwerking van persoonsgegevens. Zorg er vervolgens voor dat voor de verwerkingen welke gepaard gaan met het gebruik van LOA's en RTV's vast is gesteld of wordt voldaan aan het doelbindingsvereiste. Verzeker ook dat voor de verwerkingen van persoonsgegevens in deze applicaties de vereiste bewaartermijnen zijn vastgesteld en dat deze gegevens ook daadwerkelijk conform deze bewaartermijnen worden verwijderd.



Drag er zorg voor dat verwerkingen van persoonsgegevens welke worden uitgevoerd met LOA's en RTV's voorzien zijn van een passend beveiligingsniveau. Besteed daarin aandacht aan beveiligingsmaatregelen zoals autorisatiebeheer en de logging en monitoring van gebruikersactiviteiten.

De AP wijst vervolgens op de noodzaak om, daar waar de AVG dit vereist, risicoanalyses uit te voeren ten aanzien van de verwerkingen van persoonsgegevens welke gepaard gaan met het gebruik van LOA's en RTV's. Daarin dient de focus te liggen op de risico's voor de persoonlijke levenssfeer van belastingplichtigen. Omdat LOA's en RTV's zijn voortgebracht buiten de kaders van de reguliere IV-ontwikkeling, zijn de risico's welke het gebruik van deze applicaties voor de rechten en vrijheden van burgers waarschijnlijk groter. Deze risico's dienen te worden geïnventariseerd en waar noodzakelijk gemitigeerd.

Daarnaast beveelt de AP de Belastingdienst aan om de risico's voor de bedrijfscontinuïteit welke gepaard gaan met het gebruik van LOA's en RTV's te inventariseren en waar noodzakelijk te mitigeren. Hierbij valt te denken aan de mogelijke gevolgen van het uitvallen van een LOA of RTV voor een van de primaire processen van de Belastingdienst.

6.4.3 Kaders, regie en overzicht

De verantwoordelijkheid ten aanzien van het bestaan van LOA's en RTV's ligt nu voor een aanzienlijk deel bij de ketens. Bij het uitblijven van concrete kaders en toereikende regie leidt dit ertoe dat ketens een diffuse en niet eenduidig en gestructureerde aanpak hanteren voor een problematisch fenomeen dat binnen de gehele organisatie voorkomt. Eenduidig Belastingdienst-breed beleid is noodzakelijk om het bestaan en gebruik van LOA's en RTV's het hoofd te bieden. Hierin is naar het oordeel van de AP een rol weggelegd voor de directie IV&D.

De AP wijst de Belastingdienst op de noodzaak om de directie IV&D kaders te laten ontwikkelen ten aanzien van het gebruik van LOA's en RTV's. Daarin zou moeten onder andere moeten worden uitgewerkt aan welke eisen LOA's en RTV's moeten voldoen gedurende de periode dat ze nog niet zijn uitgezet of omgezet naar de reguliere domeinarchitectuur.

Laat de verantwoordelijke ketens ook aan IV&D rapporteren ten aanzien van de doelstelling om LOA's en RTV's te laten voldoen aan de geldende kaders.

In aanvulling op bovenstaande is het creëren van een centraal overzicht van het aantal (bedrijfskritische) LOA's dat wordt gebruikt binnen de Belastingdienst noodzakelijk om na te gaan in hoeverre de doelstelling om deze LOA's terug te dringen wordt behaald. Dat overzicht is de basis om te sturen op het terugdringen van het aantal bedrijfskritische LOA's, en om directies of ketens aan te spreken als het terugdringen van LOA's onvoldoende voortgang kent.

6.4.4 Een plan om LOA's en RTV's uit te faseren

Er dient een plan te komen waaruit blijkt binnen welke termijn LOA's en RTV's moeten worden omgezet in reguliere applicaties, of dienen te worden uitgezet. Voorkomen moet worden dat LOA's en RTV's worden beschouwd als een noodzakelijke en acceptabele tussenstap die jaren voortduurt. Het besef moet doordringen dat wanneer een LOA of RTV niet aan de regelgeving voldoet ten aanzien van de bescherming van persoonsgegevens dit ernstige risico's met zich meebrengt, en dat acties dus dringend noodzakelijk zijn om dit aan te pakken.



In het plan kunnen prioriteiten worden gesteld, waarbij gestart wordt met acties voor LOA's en RTV's waarvan de risico's voor de burgers het grootst zijn.

6.4.5 Beperk gegevensleveringen uit bronsystemen

LOA's zijn in belangrijke mate afhankelijk van de toelevering van gegevens uit bronsystemen.

Bedrijfskritische LOA's kunnen ontstaan doordat gegevens geïmporteerd kunnen worden uit bepaalde bronsystemen. De AP roept de Belastingdienst op om de feitelijke mogelijkheden tot gegevensleveringen vanuit bronsystemen te beperken. Draag er daarnaast zorg voor dat een nieuwe LOA enkel ontstaat wanneer dit door een lid van het bestuursteam dringend noodzakelijk is bevonden, en dat deze LOA voldoet aan de eisen welke voor het bestaan en gebruik van LOA's zijn opgenomen in daarvoor bestemd beleid.