Auditdienst Rijk
Ministerie van Financiën

VERTROUWELIJK

Rapport van bevindingen

Quick scan naar beheersmaatregelen en risico's OCW big data challenge

Versie 1.0

Datum 20 november 2015
Status Definitief

Colofon

Titel	Rapport van bevindingen
Kenmerk	ADR/2015/1539
Auteur(s)	dhr. dhr.
Bijlagen	1
Inlichtingen	**Auditdienst Rijk** dhr. 050- @minfin.nl

Versie	Status	Datum	Verspreid naar	Wijzigingen t.o.v. vorige versie
0.1	Concept	30-10-2015	Programmamanager en projectleiders Big Data Challenge ten behoeve van hoor en wederhoor.	Eerste opzet
0.2	Concept	05-11-2015	Programmamanager, projectleiders en gemandateerd opdrachtgevers van de Big Data Challenge.	Aanpassingen naar aanleiding van bespreking 4 november. Aanpassingen zijn aangegeven d.m.v. track changes functionaliteit.
0.9	Definitief concept	09-11-2015	Programmamanager, projectleiders en gemandateerd opdrachtgevers van de Big Data Challenge en Opdrachtgever.	Reviewcommentaar uit hoor- en wederhoor verwerkt.
0.91	Definitief concept	19-11-2015	Programmamanager, projectleiders en gemandateerd opdrachtgevers van de Big Data Challenge en Opdrachtgever.	Op basis van de managementreactie bij versie 0.9 een aantal aanpassingen doorgevoerd: • Titel gewijzigd van DUO in OCW. • Bij 3.5, vierde bullet; term "naar onze mening" verwijderd die als gevolgd van de 0.2 bespreking was toegevoegd.
1.0	Definitief	20-11-2015	Opdrachtgever en gemandateerd opdrachtgevers van de Big Data Challenge.	Aangepaste managementreactie verwerkt en rapport definitief gemaakt.

Inhoud

1 Inleiding—7
1.1 Aanleiding opdracht—7
1.2 Leeswijzer—7

2 Doel opdracht en verrichte werkzaamheden—8
2.1 Doelstelling—8
2.2 Verrichte overeengekomen werkzaamheden—8
2.3 Verspreidingskring rapportage—9

3 Bevindingen—10
3.1 Er wordt geen pseudonimisering toegepast—10
3.2 Gegevens zijn direct herleidbaar—10
3.3 Gegevens zijn indirect herleidbaar—11
3.4 Organisatorische en technische maatregelen zijn niet volledig uitgewerkt—11
3.5 Wat ons verder is opgevallen—12

4 Managementreactie—13

5 Ondertekening—14

Bijlage 1: Scope en Controle raamwerk—15

1 Inleiding

1.1 Aanleiding opdracht

Het MT OCW heeft in 2015 het initiatief opgepakt om een big data challenge te organiseren. Het doel van deze challenge is het verkennen van mogelijkheden en onmogelijkheden rondom Big Data binnen het onderwijsdomein. Het gebruik van persoonsgegevens binnen de gegevensbestanden van DUO is gebonden aan wettelijke vereisten zoals: wettelijke grondslag, doelbepaling en verwerkingsgronden.
De Functionaris Gegevensbescherming (FG) DUO en de CIO van DUO hebben een adviesmemo uitgebracht voor het toepassen van big data bij de challenge. Het memo omvat een aantal specifieke adviezen gebaseerd op de richtlijnen van het CBP voor pseudonimisering en een aantal generieke adviezen voor de te treffen maatregelen.

Het CBP stelt de volgende voorwaarden aan pseudonimisering:

1. er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;
2. er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling ("replay attack") te voorkomen;
3. de verwerkte gegevens zijn niet indirect identificerend;
4. in een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2 en 3 is voldaan;
5. de pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

Voorwaarde 4 vanuit het CBP is het laten uitvoeren van een audit (onafhankelijk oordeel) voorafgaand aan de verwerking. Dit is de directe aanleiding voor dit onderzoek.

1.2 Leeswijzer

Onze rapportage van bevindingen staat in hoofdstuk 3. Voor het verwoorden van de managementreactie is hoofdstuk 4 gereserveerd. Het doel van de opdracht en de aanpak van de quick scan staan in hoofdstuk 2.

Het rapport geeft de feitelijke stand van zaken weer per 30 oktober 2015. In gesprekken is aangegeven dat het project ondertussen verdergaat met haar activiteiten waardoor risico's en bevindingen kunnen veranderen.

2 Doel opdracht en verrichte werkzaamheden

2.1 Doelstelling

Deze opdracht is uitgevoerd in opdracht van de heer W.J.M. Westerbeek, Hoofddirecteur DUO. Het doel van het onderzoek is om te onderzoeken in hoeverre in opzet voldaan wordt aan de voorwaarden die het CBP stelt aan pseudonimisering. Het onderzoek is uitgevoerd in de vorm van een quick scan welke resulteert in dit rapport van feitelijke bevindingen. Er is gekozen voor deze aanpak doordat het project zich nog in een fase bevindt waarbij nog niet alle maatregelen in bestaan getroffen zijn. En de opdrachtgever in een kort tijdbestek een beeld wil krijgen van de getroffen maatregelen.

2.2 Verrichte overeengekomen werkzaamheden

Deze opdracht is uitgevoerd overeenkomstig de NOREA code of ethics en NOREA richtlijn 4401, "Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie." In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. Indien andere (aanvullende) werkzaamheden of assurance-opdracht zouden zijn uitgevoerd, zouden wellicht andere onderwerpen zijn geconstateerd en gerapporteerd.

Het onderzoek is uitgevoerd als quick scan, inhoudelijk bestaat de scan uit het bestuderen van (papieren en digitale) documentatie en het interviewen van relevante personen. Het onderzoek is uitgevoerd aan de hand van een controle raamwerk (bijlage 1). Dit raamwerk is tot stand gekomen door middel van een kort vooronderzoek waarbij de belangrijkste maatregelen en risico's zijn geïnventariseerd door de auditors.

De volgende projectstukken zijn gebruikt voor het onderzoek:

Document	Versie/datum
Privacy Impact Assessment (PIA)	1.1
Memo Pseudonimiseringsoplossing Big Data Challenge	1.0
Memo - big data memo aan DG en SG	23-09-2015
Teamplan data	*Geen versienr.*
Teamplan techniek	1.0
Technisch ontwerp big data test	1.0
Besluitenlijst big data	21-10-2015
Risicoanalyse informatiebeveiliging big data challenge	1.0
Gegevenswoordenboek	Concept
Gegevensleveringsovereenkomst (GLO)	Alleen template
Plan van aanpak Big data	0.2
Annotatie & Terugkoppeling PO SG-DGDUO	25-09-2015

Interviews zijn gevoerd met de volgende OCW medewerkers:

Naam	Functie/Rol
	Projectleider techniek
	Projectleider data
	Functionaris Gegevensbescherming (FG)
	Decentrale Security Officer (DSO)
	Decentrale Privacy Officer (DPO)
	Gemandateerd opdrachtgever
	Gemandateerd opdrachtgever
	Clustercoördinator DWH/cc
	Ontwikkelaar Infrastructuur
	IT-Infrastructuurarchitect

2.3 Verspreidingskring rapportage

Deze rapportage wordt uitgebracht aan de opdrachtgever van de quick scan en aan projectleden en opdrachtgevers van het project big data challenge. Verspreiding buiten die kring dient voorgelegd te worden aan de auditor.

3 Bevindingen

3.1 Er wordt geen pseudonimisering toegepast

Op basis van gesprekken, het memo pseudonimiseringsoplossing en het gegevenswoordenboek DWH is vastgesteld dat geen pseudonimisering wordt toegepast. Pseudonimiseren is het toepassen van cryptografische bewerkingen op identificerende gegevens[1]. Wat DUO onder pseudonimisering verstaat is het verwijderen van direct identificerende gegevens, met uitzondering van het unieke Datawarehouse (DWH) ID, pseudoID genaamd. Er wordt in die zin geen gebruik gemaakt van versleuteling (encryptie).

Het resultaat van deze aanpak is dat er een gegevensset gegenereerd wordt waarop de richtlijnen van het CBP ten aanzien van pseudonimisering feitelijk niet bruikbaar zijn. Een replay-attack is op deze wijze niet een risico.

3.2 Gegevens zijn direct herleidbaar

Zoals hierboven vermeld, stellen wij vast op basis van gespreken en de memo pseudonimiseringsoplossing dat vanuit DWH het veld PseudoID wordt meegegeven in de gegevenssets. Het PseudoID is een uniek identificerend nummer wat wordt toegekend zodra gegevens geladen worden in het DWH. Doordat dit nummer één op één wordt meegegeven in de gegevensset is sprake van directe herleidbaarheid.

Het CBP stelt[2] dat om te bepalen of een persoon op wie een gegeven betrekking heeft "geïdentificeerd of identificeerbaar" is in de zin van de wet er drie categorieën van gevallen te onderscheiden zijn. Bij de tweede categorie wordt een voorbeeld aangehaald ten aanzien van nummers: "*...Te denken valt aan een situatie waarbij een lijst van nummers met bijbehorende namen beschikbaar is, hetzij via openbare bron, (bijvoorbeeld het telefoonboek), hetzij via een bron die slechts raadpleegbaar is voor een bepaalde categorie van personen (bijvoorbeeld het kentekenregister door de politie of het nummer van een rekening door bankemployés). De met die nummers verbonden gegevens zijn - hoewel niet op naam - persoonsgegevens wegens de beschikbare mogelijkheid om met behulp van de nummers de identiteit van de betrokken personen te achterhalen....*"

Het PseudoID is via het DWH in principe alleen raadpleegbaar voor medewerkers van DWH/cc (plm. 30). Het aantal DUO medewerkers wat toegang kan krijgen is groter. Denk hierbij aan Database/Windows beheerders en medewerkers die toegang hebben tot de generieke accounts in de DWH database. In gesprekken is aangegeven dat het risico ten aanzien van de challengedeelnemers zeer beperkt wordt ingeschat omdat deze deelnemers geen toegang hebben tot dit ID, met uitzondering van de DWHcc medewerkers die sowieso al toegang hebben tot de gehele gegevensset. Het risico op directe herleidbaarheid bij het openbaar worden (lekken) van de dataset wordt ook als beperkt ingeschat omdat niet-DUOmedewerkers geen toegang hebben tot het PseudoID.

1 CBP Richtsnoeren – Beveiliging van Persoonsgegevens.
2 https://cbpweb.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-wbp

3.3 Gegevens zijn indirect herleidbaar

Op basis van gesprekken, gereviewde documenten (PIA en Besluitenlijst) constateren wij dat meerdere datavelden worden aangeleverd die indirecte herleidbaarheid mogelijk maken. Daarmee is feitelijk weer sprake van een persoonsgegeven in de zin van de WBP.

In de memo Pseudonimiseringsoplossingen wordt de conclusie getrokken dat door het verwijderen van de letters bij de postcode, dag bij geboortedatum en overlijdensdatum de indirecte identificeerbaarheid is tegengegaan. In het gegevensoverzicht en concept gegevenswoordenboek valt te lezen dat velden worden aangeleverd als opleiding, geboorteland ouders, leeftijd, woonplaats. Met deze gegevens is het volgens het CBP[3] mogelijk om te herleiden op natuurlijke personen.
"...Daarnaast valt te denken aan situaties waarin een bijzondere eigenschap of combinatie van gegevens hetzij direct, hetzij door koppeling of vergelijking met andere beschikbare informatie identificatie van een persoon mogelijk maakt. Een combinatie van beroep, woonplaats en leeftijd is doorgaans sterk identificerend, ook als de identiteit van betrokkene niet meteen vermeld wordt..."

Een afweging welke risico's DUO loopt ten aanzien van indirecte herleidbaarheid is beperkt verwoord. In de besluitenlijst staat dat er sprake is van indirecte herleidbaarheid. Maar ook dat er niet restrictief wordt omgegaan met data en achteraf de conclusie getrokken kan worden dat uitkomsten ongewenst zijn. Deze conclusie is niet verwoord in de PIA.

Wij hebben geen duidelijke kwantitatieve grenzen aangetroffen voor de minimale aantallen voor onder meer een bepaalde postcode zoals bijvoorbeeld een CBS die hanteert. DUO onderkent dat er een grijs gebied is bij het bepalen hoe ver te gaan ten aanzien van generaliseren. De gemaakte keuzes hierin en de mogelijke risico's zijn niet vastgelegd.

In gesprekken en de memo Pseudonimiseringsoplossingen is door het projectteam Big Data Challenge aangegeven dat het risico van indirecte herleidbaarheid beperkt wordt ingeschat doordat deelnemers aan de challenge externe informatiebronnen moeten aanwenden of kennis op voorhand moeten hebben om gegevens indirect te herleiden. In gesprekken is aangegeven dat de toegang tot externe informatiebronnen zoveel mogelijk beperkt wordt. Technisch door laptops af te schermen en organisatorisch door deelnemers niet de beschikking te geven over hun mobiele devices.

3.4 Organisatorische en technische maatregelen zijn niet volledig uitgewerkt

Op basis van het controle raamwerk hebben wij de volgende bevindingen ten aanzien van de organisatorische en technische maatregelen gedaan:

- In de stukken is geen vastlegging teruggevonden van het informeren van de DUO data-eigenaren. In gesprekken is aangegeven dat de DGDUO en SG OCW hun akkoord hebben gegeven, we hebben stukken ontvangen die een akkoord van de SG bevestigen.
- In gesprekken is aangegeven dat de schijven in de Laptops van het type SSD zijn en dat door wissen de data niet meer terug te halen zou zijn. Op basis van door ons geraadpleegde literatuur (achtergrondstuk Crypto Erase) signaleren wij dat het alleen wissen nog onvoldoende is. De Baseline Informatiebeveiliging Rijksdienst (BIR) beschrijft hoe de disks minimaal gewist moeten worden.

3 https://cbpweb.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-wbp

- Een aantal documenten verkeert op moment van onderzoek nog in conceptfase of zijn nog niet opgesteld. Door het ontbreken van de benodigde vastleggingen is het voor ADR niet goed mogelijk om vast te stellen of op adequate wijze invulling is gegeven aan de vereiste voorwaarden van het CBP. De volgende documenten waren wel verwacht maar zijn nog niet opgeleverd (en dus niet gereviewd):
    - Technische ontwerp voor laptopinrichting (inclusief hardening).
    - Protocol voor het vernietigen van de data.
    - Overeenkomst / afspraken met de geselecteerde koerier. In gesprekken is aangegeven dat dezelfde koerier als bij het transport van waardepapieren (zoals bij Examendiensten) wordt gebruikt.

3.5 Wat ons verder is opgevallen

- Voor het project is de PIA een belangrijk document. Ons valt op dat de PIA voor dit project niet conform de daarvoor beschikbare handreikingen is ingevuld. Het "Toetsmodel PIA Rijksdienst" stelt dat niet de gehele vragenlijst dient te worden gevuld. Afhankelijk van het type project zullen een aantal hoofdstukken gevuld moeten worden. De NOREA heeft een handreiking opgesteld, hieruit blijkt dat wanneer geen sprake is van persoonsgegevens (zoals in de huidige PIA verwoord) gestopt had kunnen worden na vraag 1.
- Uit diverse gesprekken blijkt dat het onderwerp privacy en beveiliging bij betrokkenen de aandacht heeft gehad. Vanaf een vroeg stadium zijn de DPO en DSO bij het traject betrokken. Uit meerdere documenten blijkt dat het project aan risico's heeft gedacht. Wij hadden echter verwacht dat er gestructureerde risicoanalyses uitgevoerd zouden zijn bij aanvang van en gedurende het project voor het bepalen van de te treffen maatregelen. In gesprekken is aangegeven dat er een meer organische vorm is toegepast.
- Tijdens het project is door de DSO een risicoanalyse vanuit informatiebeveiliging opgeleverd. Hierbij merken wij op dat de analyse is uitgevoerd met inachtneming van reeds getroffen maatregelen. Door deze gekozen uitgangssituatie verliest de risicoanalyse aan kracht, er wordt geredeneerd vanuit bestaande kaders en niet vanuit de blanco situatie.
- Bij meerdere documenten en in gesprekken is geconstateerd dat ten aanzien van de privacy geredeneerd wordt vanuit de risico's die de deelnemers aan de challenge vormen. Een belangrijk risico, het lekken of ter kennis komen aan derden zien wij niet structureel terug komen in alle documenten. Op 1-1-2016 treedt de aangepaste WBP (Meldplicht Datalekken) in werking. Deze heeft belangrijke consequenties voor het werken met big data en datalekken. Het risicoprofiel verandert o.a. vanwege meldplicht aan CBP en/of betrokkenen en hoge bestuurlijke boetes waarbij zowel de organisatie als de bestuurder aansprakelijk gesteld kunnen worden.
- In 2005 is door het CBP een (negatief) advies[4] gegeven bij aanlevering van gegevens van de toenmalige voorganger van DUO (IB-Groep) aan MinOCW en Inspectie. CBP heeft hierin een aantal adviezen gedaan ten aanzien van indirecte herleidbaarheid. Op basis van de beschrijving lijkt het alsof de Big Data Challenge een zelfde soort traject is als 11 jaar geleden. Wij hebben niet kunnen vaststellen of dit CBPadvies door DUO is meegenomen in de aanpak.

4 CBP 30 juni 2005, z2005-0528

4 Managementreactie

Opdrachtgever(s) en projectteam Big Data challenge hebben aandachtig kennis genomen van de bevindingen van de auditors. Vooral de snelheid die de onderzoekers hebben gemaakt bij het doen van hun onderzoek en rapporteren van hun bevindingen wordt gewaardeerd.

Enkele kanttekeningen en aanvullingen:

1. Aanvullende maatregelen
De concept bevindingen van de auditors hebben er binnen het project toe geleid dat aanvullende maatregelen zijn getroffen. Over het pseudo-id dat door het project in plaats van het bsn werd gehanteerd is een hash uitgevoerd waardoor er geen enkele relatie meer te leggen is tussen het identificatienummer en het bsn. Ook zijn aanvullende maatregelen getroffen op het gebied van transport en techniek om te vermijden dat –tijdens vervoer of na afloop van de challenge- gegevens te vinden zouden kunnen zijn op de harde schijven van de gebruikte apparatuur.

2. Semantiek
- Is er wel of niet sprake van pseudonimisering? De auditors houden strikt vast aan de definitie van het CBP waarin wordt gesteld dat pas sprake is van pseudonimisering na cryptografische bewerking[5]; een procesinterventie. Het projectteam heeft zich gericht op het te bewerkstelligen resultaat van pseudonimisering: gegevens die niet direct kunnen leiden tot identificatie van een persoon. Door te kiezen voor een pseudo-id en het weglaten van identificerende kenmerken in postcode is aan de pseudonimisering-eis voldaan.
- Is er al dan niet sprake van indirecte herleidbaarheid? Het auditteam stelt dat dat het geval is. Feitelijk is dat ons inziens een terechte conclusie. Tegelijkertijd stellen we vast dat die conclusie al voorafgaand aan de audit gegeven kan worden omdat nooit 100% uitgesloten kan worden dat iets indirect herleidbaar is.

3. Bereik van de audit
Moet de audit gaan over de challenge – die start nadat pseudonimisering is gerealiseerd - of over de voorbereiding van de challenge die begint met het bewerken (pseudonimiseren) van gegevens die voor een ander doel zijn verzameld, zoal bekostiging instellingen, studiefinanciering en examens?
De bevindingen van de auditors gaan over de voorbereidende bewerking van de data en over de challenge zelf. Inherent aan data-gedreven onderzoek is dat er altijd sprake zal zijn van afwijking van het doel waarvoor gegevens zijn verzameld; dat is de essentie van de onderzoeksmethode. De ironie is dat juist het voorbereiden/bewerken van persoonsdata voor gebruik in Big Data onderzoek d.m.v. pseudonimisering zodanig dat ze geen identificerende kenmerken meer heeft, op gespannen voet staat met de privacyregelgeving.

4. Feit, verwachting en verwijzing naar historie
De onderzoekers refereren aan een case die in het verleden speelde en feitelijk niet tot de scope van deze quick scan behoort. Daarnaast hoort ons inziens een verwachting van het auditteam niet thuis in dit rapport, is immers geen feit.

5. Tot slot
We hechten er aan op te merken dat de constatering rond directe herleidbaarheid ten tijde van de audit juist is maar dat deze mogelijkheid inmiddels door aanvullende maatregelen (zie ook 1) niet meer aan de orde is.

5 waar de challenge inmiddels aan voldoet, zie punt 1

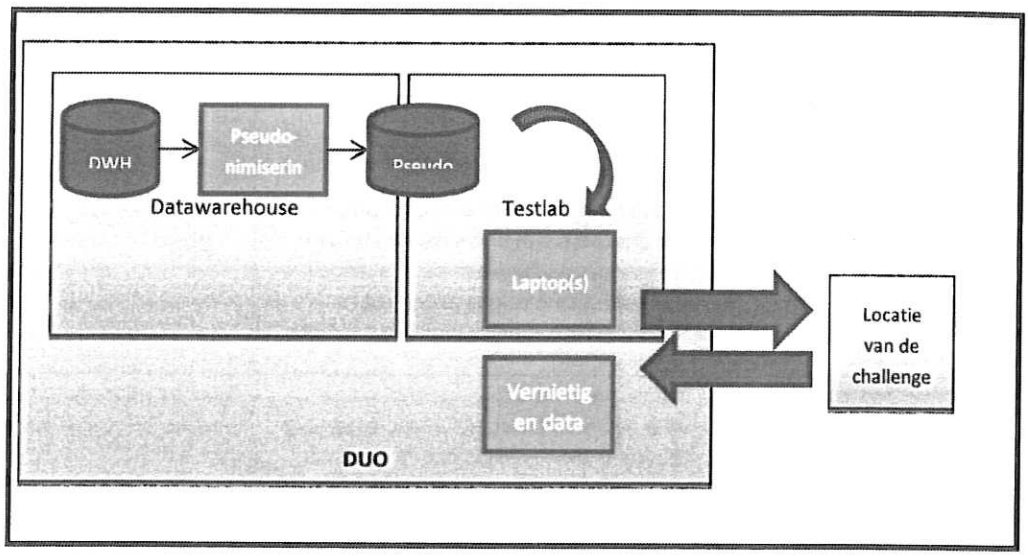
5 Ondertekening

Groningen, 20 november 2015

dhr.
Auditmanager

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag

Bijlage 1: Scope en Controle raamwerk



Nr.	Processtap	Beheersmaatregel	Risico
1	Algemeen	Data-eigenaren hebben akkoord gegeven voor het gebruik van hun data voor pseudonimisering en de challenge.	Data-eigenaren zijn verantwoordelijk voor de juiste, volledige en vertrouwelijke verwerking van Data. Wanneer zij niet tijdig hun akkoord geven dan bestaat het risico dat delen van de dataset niet gebruikt kunnen worden voor de challenge.
2	Pseudonimisering	Er wordt gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens.	Het onvoldoende pseudonimseren maakt dat de gegevensset onder de WBP valt. Het niet direct bij de bron pseudonimiseren maakt het beter mogelijk een replay attack uit te voeren.
3	Pseudonimisering	De verwerkte gegevens zijn niet indirect identificerend.	Door onvoldoende te generaliseren kan op basis van indirecte gegevens als geboortedatum, postcode, etc, gegevens herleid worden tot een natuurlijk persoon.
4	Pseudonimisering	De toegang tot de versleuteling mechaniek en hashes zijn conform BIR beveiligd.	Wanneer de versleuteling mechaniek onvoldoende beveiligd is, is de kans groter om een succesvolle replay attack uit te voeren.
5	Testlab	Het testlab voldoet aan het beveiligingsbeleid van DUO/OCW (BIR).	Door het testlab onvoldoende te beveiligen wordt kans op datalekken vergroot.
6	Laptops	Laptops worden gehardend conform een beschreven protocol.	Het risico bestaat dat enerzijds onvoldoende maatregelen getroffen zijn en anderzijds achteraf niet aantoonbaar gemaakt kan worden welke maatregelen in opzet getroffen waren.

7	Transport (heen en terug)	Laptops worden op dusdanige wijze getransporteerd dat de kans op diefstal tot een acceptabel niveau is verlaagd.	Het risico bestaat dat bij onvoldoende beveiligd transport, laptops vermist raken wat de kans op datalekken vergroot.
8	Transport (heen en terug)	Er is beschreven wie verantwoordelijk is voor de afgifte en aanname van de laptops aan en van de transporteur. Er vindt kwijting plaats.	Wanneer kwijting niet plaatsvindt kan bij vermissing van een laptop kan achteraf niet worden vastgesteld wie in bezit was van de laptop.
9	Data Challenge (Deelnemers)	Er zijn organisatorische maatregelen getroffen om datalekken te voorkomen: • Alle deelnemer hebben geheimhoudingsverklaring ondertekend. • Deelnemers zijn zich bewust van de regels die gelden voor de challenge. (Uitkomsten niet gebruiken, geen middelen meenemen om informatie te verspreiden).	Als gebruikers onvoldoende bewust zijn van geheimhouding, is de kans groter dat data of informatie gelekt wordt.
10	Data Challenge (Locatie)	De ruimte waar de challenge gehouden wordt is zowel overdag als 's nachts op een dusdanige wijze beveiligd dat de kans op datalekken beperkt is tot een voor DUO geaccepteerd niveau.	Door onvoldoende maatregelen te treffen bestaat het risico op datalekken.
11	Data Challenge	Gebruikersnamen en wachtwoorden voor de laptops worden niet op papier verstrekt.	De kans is groot dat wanneer de inloggegevens op papier verstrekt wordt dat deze bij de laptops bewaard worden, waarmee genomen beveiligingsmaatregelen teniet worden gedaan.
12	Vernietigen data	Datavernietiging gebeurd conform de door de BIR beschreven methode of zwaardere methode.	Wanneer hardware hergebruikt wordt is met tooling verwijderde data te reproduceren.
13	Vernietigen data	Van de vernietigde data wordt een proces verbaal opgesteld waarbij is beschreven welke beheerder, wanneer, welke laptop heeft gewist.	Risico bestaat dat wanneer de te nemen maatregelen niet beschreven zijn, deze niet conform afspraak uitgevoerd worden. Door het niet vastleggen van de uitgevoerde activiteiten in een PV, is achteraf niet vast te stellen dat de vernietiging van data heeft plaatsgevonden.