

Privacy Impact Assessment - LCH

Uitgevoerd volgens:
Model gegevensbeschermingseffectbeoordeling Rijksdienst
Versie 1.0, september 2017

Uitgevoerd door:	5.1.2e	5.1.2e
Versie:	8	
Datum:	25 juni 2020	
Status:	concept	

1. Voorstel.....	3
2. Persoonsgegevens.....	3
3. Gegevensverwerkingen.....	6
4. Verwerkingsdoeleinden.....	7
5. Betrokken partijen.....	7
6. Belangen bij gegevens verwerkingen.....	7
7. Verwerkingslocaties.....	7
8. Technieken en methoden van de gegevensverwerkingen.....	8
9. Juridisch en beleidsmatig kader.....	8
10. Bewaartermijnen.....	8
11. Rechtsgrond.....	8
12. Bijzondere persoonsgegevens.....	8
13. Doelbinding.....	8
14. Noodzaak en evenredigheid.....	9
15. Rechten van de betrokkenen.....	9
16. Risico's.....	10
Risico's identificeren.....	10
Categorie: zakelijke (contact)gegevens.....	10
Categorie: particulieren.....	10
Categorie: medewerker gegevens.....	10
Risico's inschatten.....	11
Fysieke informatie.....	11
Digitale informatie.....	11
Conclusie.....	11
17. Maatregelen.....	12
Bijlage A.....	13

1. Voorstel

Uitvoering van onderdeel ten behoeve van infectieziektebestrijding.

Om vraag en aanbod goed in kaart te krijgen en aan de hand daarvan de inkoop, productie, verdeling en bezorging zo efficiënt mogelijk te laten verlopen is in overleg met het ministerie van Volksgezondheid, Welzijn en Sport (VWS) het Landelijk Consortium Hulpmiddelen (LCH) opgericht.

De scope van deze PIA zijn de werkzaamheden uitgevoerd door de organisatie LCH te Leusden. Het LCH is geen zelfstandig bestuursorgaan (zbo) of een andere juridische entiteit.

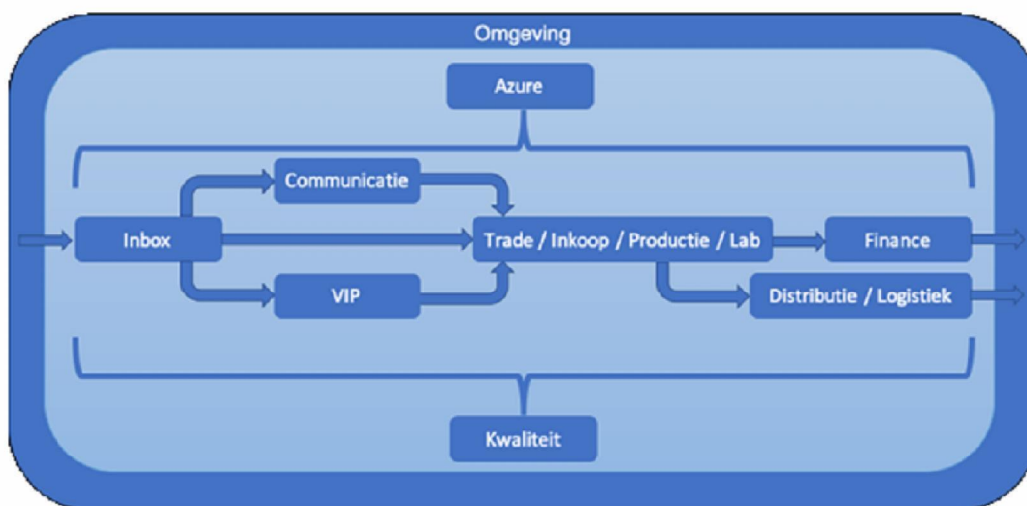
2. Persoonsgegevens

De categorieën 'bijzonder', 'strafrechtelijk' en 'wettelijk identificatienummer' worden niet gebruikt binnen de scope. Er worden wel 'gevoelige' gegevens bijgehouden. Dit geldt voor de resultaten van de creditchecks van bedrijven en de resultaten van de qualitycheck uitgevoerd op producten.

Er worden video's gemaakt door LCH die in Teams worden opgeslagen en daar alleen zichtbaar zijn voor LCH medewerkers die een Teams account hebben. Deze video's vallen niet onder de categorie 'bijzondere persoonsgegevens' aangezien video's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijk persoon mogelijk maken¹.

In tabel 1 wordt per afdeling van het LCH aangegeven welke persoonsgegevens verwerkt worden. Met uitzondering van bovengenoemde gegevens zijn dit allen 'gewone' persoonsgegevens.

Figuur 1 geeft de informatie stromen binnen het LCH weer.



Figuur 1

Tabel 1

Het (Romeinse) nummer voor de afdelingsnaam verwijst naar de overeenkomstige gegevensverwerking genoemd in hoofdstuk 3.

¹ Bron: AVG overweging 51

Afdeling	Persoonsgegevens
<i>i. Inbox (callcenter)</i>	
	• Voornaam • Achternaam • Organisatienaam (indien van toepassing) • Email adres
<i>ii. Productie (Nederland) / Inkoop (Europa) / Trade (Azië)</i>	
	• Organisatienaam • Voornaam en achternaam contactpersoon • Functie contactpersoon • Telefoonnummer zakelijk • E-mailadres zakelijk • KvK-nummer • Extern onderzoeksrapport product ○ Goedkeuring/afkeuring ○ Leverancier en productnaam is geanonimiseerd
<i>iii. Lab (testlijn)</i>	
	• Offertes • Contracten • Orders • Leveranciersoverzicht Voor al deze gegevensverzamelingen geldt dat wordt bijgehouden: • Organisatienaam • Voornaam en achternaam contactpersoon • E-mailadres zakelijk • Telefoonnummer zakelijk • KvK-nummer (wordt niet bijgehouden in het leveranciersoverzicht)
<i>iv. Finance</i>	
	• Organisatienaam • Voornaam en achternaam contactpersoon • Telefoonnummer • E-mailadres • KvK-nummer • Rekeningnummer (IBAN) • Kredietcheck bedrijf • Bedrijfsgegevens kunnen gelijk zijn aan prive gegevens zoals woonadres en prive rekeningnummer)
<i>v. Logistiek</i>	
	• Organisatienaam

	• Voornaam en achternaam contactpersoon • Functie contactpersoon • Telefoonnummer • E-mail adres zakelijk
<i>vi. Distributie</i>	
	• Contract en Urenggegevens van inhuur ○ Voornaam en achternaam ○ Organisatienaam ○ Kvk nummer ○ Telefoonnummer ○ Email adres ○ Reisafstand (en indirect adresgegevens) • Registratiegegevens / ingangstoegangscontrole ○ Uren per dag(deel) • Contracten voor opslag ○ NAW ○ Organisatienaam ○ Tarief • Transport en warehouse contracten ○ Toeleveranciers worden via een andere partij gecontracteerd (stellingen/DHL/CB/PostNL/...) • Vraag naar Alex over presentatie met partners
<i>vii. Communicatie</i>	
	• Maillinglijst ○ E-mail adres
<i>viii. Kwaliteit</i>	
	• Organisatienaam
<i>ix. Fysieke beveiliging</i>	
	• Bezoekersregistratie Bezoekers Leusden en Vianen. Op andere locaties wordt dit niet bijgehouden. Op de twee nieuwe locaties in Tiel en Rotterdam gaat er wel een bezoekersregistratie bijgehouden worden. CB doet de logistiek vanuit de warehouses ○ Voornaam en achternaam bezoeker ○ Organisatie ○ Datum en tijdstip binnenkomst ○ Tijdstip vertrek
<i>x. Facilitair</i>	
	• Leveranciers

	○ Contract en Urengegevens van inhuur ○ Naam ○ Organisatienaam ○ Kvk nummer ○ Telefoonnummer ○ Email adres ○ Reisafstand (en indirect adresgegevens)
<i>xi. VIP</i>	
	● Voornaam en achternaam ● Naam organisatie (is soms de naam waarop de VIP publiekelijk bekend is) ● Contactpersoon bij VWS/LCH ● Telefoonnummer ● E-mailadres
<i>xii. ICT beheer: LCH data onder beheer van Delta-N</i>	
	Gewone persoonsgegevens: ● LCH medewerkers met een gebruikersaccount in Team: ● Voornaam en achternaam ● Email adres ● Telefoonnummer ● Bedrijfsnaam

3. Gegevensverwerkingen

-
- i. Inbox (callcenter)
 - Telefonische contacten documenteren
 - Outlook mailbox waarin binnengekomen mails worden bewaard.
-
- ii. Productie (Nederland)/ Inkoop (Europa) / Trade (Azië)
 - Contactgegevens contactpersoon producten
 - Gegevens voor het opstellen voor contracten.
 - Gegevens voor het opstellen van orderformulieren
 - Extern onderzoeksrapport product
-
- iii. Lab (testlijn)
 - Contactgegevens contactpersoon testen
 - Gegevens voor het opstellen voor contracten.
 - Gegevens voor het opstellen van orderformulieren
-
- iv. Finance
 - Verwerken van facturen
 - Kredietcheck bedrijf
 - Opbouwen financieel archief
-
- v. Logistiek
 - Verificatie facturatie
 - Quality check ingekochte goederen

- Inklaren en transport goederen naar Nederland, en binnen Nederland
-
- vi. Distributie
 - Contracten voor distributeurs
 - Contracten voor opslag producten
 - Registeren van toegangscontrole
 - Contracten voor warehouse en transport
- vii. Communicatie
 - Bijhouden van e-mail adressen voor mailinglijst t.b.v. nieuws over updates.
(noot: posts op social media is de taak van VWS)
- viii. Kwaliteit
 - Overzicht van organisatie namen
- ix. Fysieke beveiliging
 - Bezoekersregistratie bedrijfspand Leusden, Vianen, Tiel en Rotterdam
- x. Facilitair
 - Contracten voor inhuur
 - Uitbetaling loon en reiskostenvergoeding personeel
- xi. VIP
 - Overzicht van contactpersonen
- xii. ICT beheer: LCH data onder beheer van Delta-N
 - Accountbeheer medewerkers
 - LCH video's
 - Databeheer LCH

4. Verwerkingsdoeleinden

Uitvoering van onderdeel ten behoeve van infectieziektebestrijding.

Om vraag en aanbod goed in kaart te krijgen en aan de hand daarvan de inkoop, productie verdeling en bezorging zo efficiënt mogelijk te laten verlopen is in overleg met het ministerie van VWS het LCH opgericht.

5. Betrokken partijen

Verwerkingsverantwoordelijke	Verwerker	Verstrekker	Ontvanger
Minister VWS / SG VWS ² namens het Ministerie van	Het Landelijk Consortium	• Potentiële klanten • Klanten	• Intern Landelijk Consortium

² Doorhalen wat niet van toepassing is

Volksgezondheid, Welzijn en Sport (VWS)	Hulpmiddelen (LCH)	• Leveranciers • Medewerkers	Hulpmiddelen (LCH) • Leveranciers • (Potentiële) klanten
---	--------------------	---	---

6. Belangen bij gegevens verwerkingen

- - Reguleren van de inkoop en verkoop van persoonlijke beschermingsmiddelen in Nederland om mogelijke tekorten in de zorg tegen te gaan.
 - Het voorkomen van onrust in de maatschappij.
 - De klanttevredenheid te waarborgen.
 - Het functioneren van de medewerkers te bevorderen.
 - Het voldoen van betalingen en facturen.

7. Verwerkingslocaties

Voor alle gegevensverwerkingen binnen LCH geldt dat de verwerking plaatsvindt in Nederland. Azure is zo geconfigureerd dat alle dataopslag plaatsvindt in Europa.

8. Technieken en methoden van de gegevensverwerkingen

Er is geen sprake van:

- (semi)geautomatiseerde besluitvorming
- Profiling
- Big-data verwerkingen

9. Juridisch en beleidsmatig kader

•
Relevante aanvullende wetgeving naast de AVG en de Richtlijn:

- Belastingwetgeving (voor het bijhouden van een deugdelijke financiële administratie).

10. 10. Bewaartermijnen

Tenzij hieronder anders vermeldt is de bewaartermijn voor alle documenten zeven jaar. Dit sluit aan bij de gangbare (belasting)praktijk.

11. 11. Rechtsgrond

Taak van algemeen belang.

Nederland heeft te maken met een epidemie van het coronavirus SARS-COVID-2. Dat is een virus dat bij de meeste mensen een milde verkoudheid (en soms niet eens dat) veroorzaakt, maar sommige mensen worden er erg ziek van en moeten opgenomen worden in het ziekenhuis. Het zorgpersoneel moet beschermende kleding, mondkapjes en handschoenen dragen om mensen te testen en zieke mensen te verplegen.

12. 12. Bijzondere persoonsgegevens

Er worden geen bijzondere persoonsgegevens verwerkt.

13. 13. Doelbinding

LCH verzamelt en verwerkt de persoonsgegevens alleen voor de uitoefening van haar oorspronkelijke taak: de inkoop, test, transport en distributie van medische hulpmiddelen t.b.v. SARS-COVID-2.

14. 14. Noodzaak en evenredigheid

Veruit de meeste gegevens die worden verzameld hebben betrekking op organisaties.

In een beperkt aantal gevallen worden ook gegevens van particulieren verzameld. Dit betreft dan particulieren die suggesties doen waar medische hulpmiddelen te verkrijgen zijn.

15. 15. Rechten van de betrokkenen

Verzoeken van betrokkenen worden ontvangen door de afdeling Inbox. De afdelingen Inbox, VIP en medewerkergegevens hebben als enige te maken persoonsgegevens van individuen.

De verzoeken³ van individuen worden altijd gehonoreerd tenzij hun contactmoment heeft geleid tot een zakelijke transactie. In dat geval kunnen de rechten van het individu worden beperkt op grond van de belastingwetgeving.

³ Recht op inzage, rectificatie, gegevenswissing, overdraagbaarheid.

16. Risico's

Risico's identificeren

Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoon.

De impact voor personen wordt hieronder beschreven. Daarin zijn de volgende groepen van betrokkenen onderkend:

- Zakelijke (contact)gegevens
- Particulieren
- medewerkers

Categorie: zakelijke (contact)gegevens

De meeste teams houden zakelijke contactgegevens bij van de personen waarmee zij contact hebben bij die organisatie. Dat een contactpersoon werkt bij een bepaalde organisatie is vaak beschikbaar op publieke bronnen zoals LinkedIn.

Een privacyincident zal dan ook *zeer beperkte* gevolgen hebben voor de betrokkenen.

Er worden ook gevoelige gegevens bijgehouden: de resultaten van de kreditchek en de resultaten van de test van de productkwaliteit.

Kreditchek:

De kreditchek wordt ingekocht bij een extern bureau dat gegevens uit publieke bronnen combineert.

Een privacyincident zal dan ook *geen* gevolgen hebben omdat die gegevens al openbaar zijn.

Testresultaten productkwaliteit:

Bij een privacyincident kan de producent in verlegenheid worden gebracht indien de testresultaten in de openbaarheid komen. Vooral als blijkt dat de testen op alle producten van één producent negatief waren.

Een privacyincident op de testresultaten kan dan ook een *gemiddelde* impact hebben.

Categorie: particulieren

De teams Inbox en VIP verwerken persoonsgegevens van particulieren die contact zoeken met de LCH.

Het VIP team handelt de communicatie af met particulieren die een politieke functie hebben of een Bekende Nederlander (BN-er) zijn.

Een deel van die personen heeft zelf publiekelijk bekend gemaakt dat zij medische hulpmiddelen beschikbaar willen stellen. Een privacyincident heeft in dat geval *geen impact* omdat het niet zal leiden tot informatie die niet eerder bekend was.

Indien de gegevens van de VIP niet eerder publiekelijk bekend waren, kan een privacyincident een *negatief gevolg* hebben voor de betrokkenen, bijvoorbeeld indien ze ervoor gekozen hebben om anoniem te blijven.

Categorie: medewerker gegevens

De teams Fysieke Beveiliging en ICT Beheer houden persoonsgegevens bij van individuen, te weten medewerkers van LCH.

Een privacyincident zal *zeer beperkte gevolgen* hebben voor de betrokkenen gezien de aard van de gegevens.

Risico's inschatten

Deze paragraaf analyseert de kans op een incident.

Fysieke informatie

In het LCH pand is informatie op papier aanwezig. Dit pand wordt 24 uur/dag bewaakt – inclusief drone detectie – zodat de *kans* op een inbraak *laag* is. De impact van een inbraak is moeilijk in te schatten omdat niet duidelijk is welke informatie op dat moment fysiek aanwezig is en gestolen dan wel gekopieerd wordt.

Digitale informatie

De bulk van de digitale informatie is opgeslagen in de Azure cloud en/of op computers van de medewerkers. De *kans* dat de gegevens in de Azure cloud wordt buit gemaakt is *gering* omdat die omgeving continue wordt bewaakt. Indien die gegevens zijn in te zien door onbevoegden is de impact *beperkt* doordat er veruit de meeste persoonsgegevens bestaan uit zakelijke contactgegevens. De impact is *gemiddeld* indien de testresultaten van producten – geclassificeerd als 'gevoelig' – in de openbaarheid komen. De testresultaten worden opgeslagen in Teams in de Azure cloud.

De *kans* dat gegevens opgeslagen op de computers van de medewerkers lekken is *gemiddeld*. Verlies of diefstal van een laptop komt regelmatig voor. Daarnaast is er een kans dat medewerkers van LCH bewust worden aangevallen. De impact zal hier beperkt blijven tot de opgeslagen persoonsgegevens. Als de informatie versleuteld is opgeslagen zal er *geen impact* als de sleutel veilig is opgeslagen. Als de informatie niet versleuteld is opgeslagen zal de *impact beperkt* zijn doordat veruit de meeste persoonsgegevens bestaan uit zakelijke contactgegevens.

Conclusie

Bij zowel de fysieke als de digitale informatie zullen de negatieve gevolgen voor de rechten en vrijheden van de betrokken *beperkt* zijn doordat de meeste persoonsgegevens bestaan uit zakelijke contactgegevens.

De combinatie van kans en impact zoals hierboven beschreven resulteert in een Laag risico.

17. Maatregelen

Aangezien het risico Laag is kunnen de maatregelen beperkt blijven tot de volgende:

- Het inrichten van een basisniveau van informatiebeveiliging in lijn met de Baseline Informatiebeveiliging Overheid (BIO) voor de Azure cloud omgeving waar ook de data uit Microsoft Teams in wordt opgeslagen. Hierbij wordt BIO BBN1 niveau zoveel mogelijk gevolgd en wordt er in een aantal gevallen ook voldaan aan het BBN2 niveau. In bijlage A staat een overzicht van de geïmplementeerde maatregelen.
- Opgeslagen video's worden verwijderd na 10 werkdagen⁴.

Ook als bovenstaande maatregelen zijn geïmplementeerd blijft er een restrisico. De onderstaande restrisico's zijn onderkend:

- Kwetsbaarheid in Azure dat wordt benut;
- Interne LCH video(s) die uitlekken naar de media.

⁴ Vanaf 19 juni 2020 zijn de meeste medewerkers al niet meer werkzaam bij LCH waardoor het in de praktijk lastig uitvoerbaar is om (achteraf) expliciet toestemming te vragen om gefilmd te worden.

18. Bijlage A

Deze bijlage geeft aan welke van de maatregelen uit BIO hoofdstuk 12 (“Beveiliging bedrijfsvoering”) zijn geïmplementeerd binnen LCH. Dit is gebaseerd op een interview met de LCH beheerder.

De scope van de onderstaande vragen betreft alleen de Azure cloud omgeving.

Niet tot de scope horen de laptops van de medewerkers. Dit zijn BYOD's die buiten het beheer en toezicht vallen van de LCH beheerders.

Samenvatting:

Van de 27 niveau BBN-1 maatregelen en de 11 niveau BBN-2 maatregelen uit hoofdstuk 12 zijn er 18 BBN-1 en 3 BBN-2 maatregelen geïmplementeerd.

12.1.1	1	Gedocumenteerde bedieningsprocedures Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Ja
12.1.2	1	Wijzigingsbeheer Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Ja
12.1.2.1	1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: a. het administreren van wijzigingen; b. risicoafweging van mogelijke gevolgen van de wijzigingen; c. goedkeuringsprocedure voor wijzigingen.	Ja
d. Handreiking: Samenhang beheersprocessen en informatiebeveiliging			
12.1.3	1	Capaciteitsbeheer f. Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	g. h. Ja
12.1.4	k.	Scheiding van ontwikkel-, test- en productieomgevingen Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	l. m. Ja n.
12.1.4.1	v.	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	o. p. Ja q.
12.1.4.2	y.	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	r. s. Ja

12.2.1	cc. Beheersmaatregelen tegen malware	ee.	
	dd. Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	ff. Ja	
		gg.	
		hh.	
	ww. Handreiking: Implementatie van detectieoplossingen	ii.	
		jj.	
12.2.1.1	zz. Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	kk. Ja	
		ll.	
12.2.1.2	aaa. Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	mm. Ja	
12.2.1.3	bbb. Gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	nn.	
		oo. Ja	
12.2.1.4	ccc. De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	pp.	
		qq. Nee	
12.2.1.5	ddd. Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: a. Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. b. Bijlagen en downloads vóór gebruik.	rr.	
		ss.	
		tt.	
		uu.	
	eee. De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	vv. Nee	
12.3.1	g.h. Back-up van informatie	j.	Deels.
	i.1.1.1. Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	k.	Backups worden wel gemaakt, niet getest.
	x. Handreiking: Back-up and recovery	l.	
12.3.1.1	z. aa. Er is een back-upbeleid waarin de eisen voor het 1 bewaren en beschermen zijn gedefinieerd en vastgesteld	m.	
		n.	Nee
12.3.1.2	ccdd. Op basis van een expliciete risicoafweging is bepaald wat het 1 maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	o.	
		p.	Nee
12.3.1.3	ff. gg. In het back-upbeleid staan minimaal de volgende eisen: 2 a. Dataverlies bedraagt maximaal 28 uur. b. Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	q.	
		r.	Nee
		s.	
		t.	
12.3.1.4	d. e. Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij 2 een incident op de ene locatie niet kan leiden tot schade op de andere.	u.	Nee
		v.	
12.3.1.5	g. h. De restore procedure wordt minimaal jaarlijks getest of na 2 een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	w.	Nee

12.4.1	j. k. Gebeurtenissen registreren	n.	
	l. Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	o. Ja	
		p.	
	II. Handreiking: Loggingbeleid	q.	
		r.	
	mm. Handreiking: NCSC-handreiking detectieoplossingen	s.	
1. 12.4.1.1 oo. pp.	Een logregel bevat minimaal:	t. Ja	
	1 a. de gebeurtenis;	u.	
	b. de benodigde informatie die nodig is om het incident methoge mate van zekerheid te herleiden tot een natuurlijk persoon;	v.	
	c. het gebruikte apparaat;	w.	
	d. het resultaat van de handeling;	x.	
	e. een datum en tijdstip van de gebeurtenis.	y.	
12.4.1.2	g. h. Een logregel bevat in geen geval gegevens die tot het 1 doorbreken van de beveiliging kunnen leiden.	z. Ja	
		aa.	
12.4.1.3	j. k. De informatieverwerkende omgeving wordt gemonitord door een SIEM en/ of 2 SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen l. gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	bb.	
		cc. Nee	
		dd.	
		ee.	
12.4.1.4	n. o. Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze 2 binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of p. via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	ff.	Nee
		gg.	
		hh.	
		ii.	
12.4.1.5	r. s. De SIEM en/of SOC hebben heldere regels over wanneer een incident 2 moet worden gerapporteerd aan het verantwoordelijk management.	jj.	
		kk.	Nee
12.4.2	u. v. Beschermen van informatie in logbestanden	x.	
	w. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Nee	
		y.	
1. 12.4.2.1 ii. jj.	Er is een overzicht van logbestanden die worden gegenereerd. 1	z. Ja	
		aa.	
1. 12.4.2.2 ll. mm.	Ten behoeve van de loganalyse is op basis van een expliciete 1 risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	bb.	Nee
		cc.	
1. 12.4.2.3 oo. pp.	Er is een (onafhankelijke) interne audit procedure die 2 minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	dd.	Nee
		ee.	
		ff.	
1. 12.4.2.4 rr. ss.	Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe 2 worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	gg.	Nee
12.4.3	1 Logbestanden van beheerders en operators	vv.	
	uu. Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	ww.	Ja
12.4.4	1 Kloksynchronisatie	zz.	
	yy. De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomen behoren te worden gesynchroniseerd met één referentietijdbron.	aaa.	Ja

pb.	12.5.1	1	Software installeren op operationele systemen	ddd.	Ja
ccc.	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.				
pe.	12.6.1	1	Beheer van technische kwetsbaarheden	ggg.	
fff.	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.			hhh.	
				iii.	Nee
				jjj.	
				kkk.	
	ooo.		Handreiking: Penetratietesten	lll.	
ppp.	12.6.1.1	1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC- classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op	mmm.	
qqq.	basis van een expliciete risicoafweging mitigerende maatregelen getroffen.			nnn.	Nee
r.	12.6.2	1	Beperkingen voor het installeren van software	ttt.	
sss.	Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.			uuu.	Ja
				vvv.	
xxx.	12.6.2.1	2	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	www.	Ja
y.	12.7.1	1	Beheersmaatregelen betreffende audits van informatiesystemen	aaaa.	
zzz.	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.			bbbb.	Nee