Publiek

CONCLUSION

RICHTLIJN LEVERANCIERS & CONTRACTMANAGEMENT

Auteur
Roel Gloudemans
(roel.gloudemans@conclusion.nl)

Met medewerking van
Chris Gralike, Ricky Hoots, Artien Bel, Dennis Pieterse, Paul Schoorl, Manfred Anneveld

Status: Definitief
Versie: 1.5 (10/05/2024 10:50)
Ten minste houdbaar tot: 2025-05-10

Versietabel			
Datum	Versie	Door	Aanpassing
21-11-15	0.1	R. Gloudemans	Eerste concept
22-02-23	1.0	R. Gloudemans	Definitief
22-10-04	1.1	R. Gloudemans	R-LM-02a, uitbreiding op R-LM-02 met landen en organisaties waartegen sancties genomen zijn.
22-10-20	1.2	R. Gloudemans	Toevoeging SBOM (R-LM-29 en R-LM-30)
22-12-15	1.3	R. Gloudemans	Aanpassing aan ISO27001:2022, verwijdering mapping tabel
23-04-12	1.4	R. Gloudemans	Aanpassing R-LM-03, toegevoegd dat het certificaat van een geaccrediteerde instantie moet zijn.
24-05-10	1.5	R. Gloudemans	Update eis naar ISO27001:2022

Accordering	
Document	Versie
Versie	1.0
Alle hoofdversies van dit document worden geaccordeerd door minimaal 5 security officers van verschillende Conclusion bedrijven. Kleine wijzigingen, zoals spelfouten en wijzigingen en/of aanvullingen op de toelichting vinden plaats onder de verantwoordelijkheid van de Chief Security Officer van Conclusion	
*Dit document is geclassificeerd als **publieke** informatie en kan (in pdf-vorm) beschikbaar worden gesteld aan iedereen voor wie dit beleidsstuk mogelijk relevant is.*	

Inhoud

1. Inleiding

Conclusion is voor haar dienstverlening afhankelijk van ingekochte diensten en producten van anderen. Het is daarom belangrijk dat het veiligheidsniveau van deze ingekochte diensten aansluit bij de beveiliging van Conclusion zodat er een sterke en weerbare dienstenketen ontstaat. Zogenaamde “supply chain” aanvallen kunnen alleen voorkomen worden door een goede samenwerking tussen leverancier en afnemer. Hierbij hoort het stellen van duidelijke eisen.

De eisen die aan de leveranciers en producten gesteld worden zijn afhankelijk van het doel waarvoor Conclusion ze gebruikt. Een eis voor bijvoorbeeld een ISO-certificering is zinnig voor een leverancier die data verwerkt voor, of uit naam van Conclusion en/of haar klanten, maar zinloos voor de leverancier van koffiebekertjes.

1.1 Scope

De richtlijnen uit dit document zijn alleen van toepassing op partijen die bij het leveren van hun dienstverlening mogelijk de vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens die Conclusion onder haar beheer heeft kunnen beïnvloeden.

Het gaat in de praktijk om alle leveranciers die:

- waarmee een verwerkersovereenkomst afgesloten moet worden, omdat zij:
  - gegevens van medewerkers verwerken (of opslaan) of
  - gegevens van klanten van Conclusion op hun systemen opslaan en/of acteren op basis van die gegevens.
- die data verwerken of opslaan die over de interne bedrijfsvoering van Conclusion gaat.

Denk hierbij bijvoorbeeld niet alleen aan leveranciers van SaaS-diensten en hosting partijen, maar ook een communicatiebureau dat een medewerkers enquête opzet.

Deze richtlijn is een aanvulling op het geldende inkoopbeleid, zoals dat gehanteerd wordt door het betreffende Conclusion bedrijf.

1.2 Doelstelling

De doelstelling van de richtlijnen voor Leveranciersmanagement is het waarborgen van de veiligheid van data en eigendom van de organisatie, alsmede de veiligheid en gezondheid van het personeel.

Deze richtlijn maakt onderdeel uit van het beveiligingsbeleid van het Conclusion ecosysteem bestaande uit:

- Beveiligingsbeleid ecosysteem.
- Stelsel van richtlijnen, waarvan deze richtlijn er een is.

1.3 Doelgroep

De doelgroep van dit document is eenieder die een rol speelt bij de inkoop van producten en diensten binnen de scope van dit document.

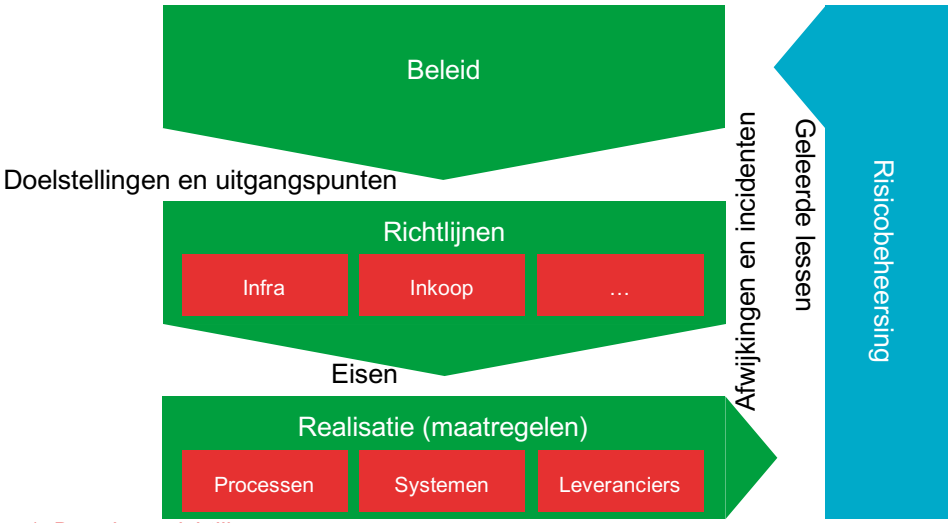
1.4 De rol van richtlijnen

De richtlijnen bij Conclusion geven de geadviseerde set van maatregelen aan, eventueel gekoppeld aan de classificatie van de data. Sommige van de richtlijnen zijn direct in te

vullen, anderen moeten door architecten en ontwerpers verder uitgewerkt worden voor de context waarin de richtlijn moet worden toegepast.

Ieder bedrijf binnen Conclusion is zelf verantwoordelijk voor het vinden van de juiste balans tussen risico's nemen en mitigeren. Dit document helpt bij dat proces. De richtlijnen zijn binnen Conclusion een gemeenschappelijke set van best practises. Het niet voldoen aan een best practise moet als een kwetsbaarheid worden beschouwd en expliciet geadresseerd worden in de risicobeheersing van het bedrijf. Hieruit zal dan blijken of er daadwerkelijk een risico is en of dit risico acceptabel is.

Indien een kwetsbaarheid tot een onacceptabel risico leidt voor Conclusion moeten er stappen genomen worden deze kwetsbaarheid weg te nemen. De CSO zal de set van richtlijnen periodiek herijken op basis van de risicoanalyses van de bedrijven. Zo zullen bij een herijking van dit document overbodige richtlijnen verdwijnen uit het beleid en zullen andere toegevoegd worden.



Figuur 1, De rol van richtlijnen

2. Eisen aan leveranciers

Leveranciers kunnen producten en diensten leveren aan Conclusion. In beide gevallen is het van belang dat Conclusion op deze leveranciers kan vertrouwen voor de scope van de dienstverlening. De criteria die gehanteerd worden om een partij te kunnen vertrouwen nemen toe met het belang van de data en diensten van Conclusion die de leverancier mogelijk kan beïnvloeden.

Bij het leveren van diensten hoeft alleen de leverancier zelf beschouwd te worden. Bij afname van een product moeten zowel leverancier als fabrikant geëvalueerd worden. Onderstaande tabel geeft aan wanneer een leverancier/fabrikant vertrouwd kan worden. Hierbij is rekening gehouden met de classificatie van de data die door inzet van de dienst of product mogelijk beïnvloed kan worden. Deze richtlijnen worden aangevuld met de richtlijnen uit hoofdstuk 4 “Eisen aan producten” of hoofdstuk 5 “Eisen aan diensten”.

In de onderstaande tabel worden de maatregelen weergegeven. Bij iedere maatregel staat een classificatie aangegeven. *De classificatie heeft betrekking op vertrouwelijkheid, integriteit of beschikbaarheid.* De zwaarste classificatie is de classificatie die telt.

Alle dataclassificatie niveaus van Conclusion			
Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
1	Zeer laag	Niet gecontroleerd	Publiek
2	Laag	Correct	Bedrijfsgegevens
3	Midden	Belangrijk	Intern
4	Hoog	Essentieel	Vertrouwelijk

De betekenis van de classificaties is te vinden in de “Richtlijn Dataclassificatie”

Eisen aan de leveranciers					
#	**Maatregel & Toelichting**	**1**	**2**	**3**	**4**
R-LM-01	**De scope van het vertrouwen moet expliciet omgeschreven zijn.** Een leverancier wordt alleen vertrouwd voor de context waarin hij zijn product of dienst levert. Deze scope moet expliciet omgeschreven worden, inclusief de gegevens die binnen de scope worden verwerkt en de classificatie van deze gegevens. Hierbij dienen ook de voorwaarden voor dit vertrouwen vastgelegd te zijn. Deze voorwaarden bestaan uit de richtlijnen uit dit document en eventuele specifieke aanvullende maatregelen.	X	X	X	X

Eisen aan de leveranciers					
#	**Maatregel & Toelichting**	**1**	**2**	**3**	**4**
R-LM-02	**Alleen leveranciers met een goede naam.** Alleen leveranciers met een goede naam zijn toegestaan. Dit zijn leveranciers die: 1. Niet veroordeeld zijn voor of bewezen deelgenomen aan het leveren van data of toegang geven tot klantgegevens of infrastructuur aan derde partijen, buiten de Nederlandse of Europese wetgeving om. 2. In de afgelopen 5 jaar niet beboet door de Autoriteit Persoonsgegevens voor het onzorgvuldig behandelen van persoonsgegevens of het overtreden van de AVG, 3. Leverancier moet een VOG-RP kunnen overleggen. https://www.justis.nl/producten/vog/vog-voor-rechtspersonen.aspx 4. Leverancier moet bereid zijn zich te conformeren aan de AVG.			X	X
R-LM-02a	**Leverancier staat niet op of is niet gevestigd in landen van de zwarte lijst of gebruikt producten en/of onderleveranciers op de zwarte lijst.** De zwarte lijst bestaat uit landen waartegen op nationaal of op Europees niveau sancties genomen zijn als gevolg van het respecteren van de rechten van de mens, de persvrijheid of vrijheid van meningsuiting. Denk hierbij aan Rusland, Noord-Korea en Iran		X	X	X
R-LM-03	**Leverancier moet in het bezit zijn van een ISO27001:2022 certificaat of gelijkwaardig** De leverancier heeft een expliciet mechanisme om zichzelf te verbeteren. Alternatief zijn bijvoorbeeld NEN-7510:2011 en ISAE-3000. Let hierbij op het feit of het certificaat door een geaccrediteerde instantie is uitgegeven. Dit is te controleren op http://www.rva.nl De leverancier dient hiervoor jaarlijks het certificaat en “statement of applicability” te tonen, zodat de scope van de certificering duidelijk is en duidelijk is welke maatregelen uit de Annex A van toepassing zijn.			X	X
R-LM-04	**Leveranciers worden minimaal jaarlijks beoordeeld.** Alle leveranciers worden minimaal jaarlijks gecontroleerd op het voldoen aan de gestelde eisen.			X	X
R-LM-05	**Voor ieder inkooptraject moet aan de security officer om advies gevraagd.** Voordat een IT-inkooptraject wordt gestart, moet hiervoor advies ingewonnen worden de security officer, zodat		X	X	X

Eisen aan de leveranciers					
#	Maatregel & Toelichting	1	2	3	4
	deze kan beoordelen of de betreffende dienst of product past in de context van Conclusion. Voor dit advies zal de security officer bijvoorbeeld controleren of aan privacy en security by design uitgangspunten voldaan is.				

3. Eisen aan producten

Eisen aan producten					
#	Maatregel & Toelichting	1	2	3	4
R-LM-06	**Er is ondersteuning gedurende de complete lifecycle.** Indien het product afhankelijk is van firm- of software, dient deze gedurende de economische levensduur ondersteund te worden.	X	X	X	X
R-LM-07	**Kritieke kwetsbaarheden in firm- of software worden in de regel binnen enkele dagen opgelost.** Bepaal vooraf wat deze termijn dient te zijn in relatie tot de impact van eventuele kritieke kwetsbaarheden.		X	X	X
R-LM-29	**Leverancier levert een Software Bill of Materials aan (SBOM).** Op een Software Bill of Materials wordt gespecificeerd van welke software modules van derde partijen het product afhankelijk is. Dit geldt zowel voor software als hardware die voorzien is van firmware. De SBOM stelt Conclusion in staat om snel te inventariseren bij een Log4J type event.		X	X	X
R-LM-08	**Er kan een support contract afgesloten worden.** Indien het functioneren van de component essentieel is voor de Conclusion dienstverlening dient de mogelijkheid van een onderhoudscontract te bestaan. Binnen dit onderhoudscontract moet soft- en hardware ondersteuning mogelijk zijn.		X	X	X
R-LM-09	**Security tests zijn toegestaan** Sommige producten staan het doen van security en performance tests vanuit de licentie niet toe. Conclusion vindt dat niet acceptabel.			X	X
R-LM-10	**Product stuurt zonder toestemming geen data naar leverancier of derde partij.** Producten mogen alleen met expliciete toestemming data versturen naar de leverancier of derde partijen.		X	X	X
R-LM-11	**Indien product privacygevoelige data doorstuurt op opslaat, is een verwerkersovereenkomst verplicht.** Een verwerkersovereenkomst (of iets dat daar gelijkwaardig aan is) is verplicht bij het doorsturen of opslaan van privacygevoelige data.			X	X

4. Eisen aan diensten

Eisen aan diensten					
#	Maatregel & Toelichting	1	2	3	4
R-LM-12	**Leverancier staat audits toe** Leverancier staat toe dat Conclusion audits uitvoert op de infrastructuur en dienstverlening of laat dit doen door een (onafhankelijke) derde partij uit de markt, waarbij Conclusion inzicht krijgt in het audit rapport.			X	X
R-LM-13	**Leverancier heeft ISAE 3402 type II verklaring** De leverancier kan ieder jaar een ISAE 3402 type II verklaring overhandigen, voor de scope van dienstverlening. Een SOC2 type II rapport volstaat ook.			X	X
R-LM-14	**Leverancier staat security/pentests toe** Leverancier staat het toe dat Conclusion beveiligingstests uitvoert of uit laat voeren. Indien gewenst zal Conclusion deze zo uitvoeren dat verstoringen als gevolg hiervan onwaarschijnlijk zijn.			X	X
R-LM-15	**De leverancier heeft Security Monitoring voor de scope van de dienstverlening ingericht** De leverancier is voor de dienstverlening aangesloten op een eigen of ingehuurd Security Operations Centre. Alternatief is de leverancier bereid mee te werken aan een koppeling aan het SOC van het betreffende Conclusion bedrijf.				X
R-LM-16	**Dienst is te koppelen aan het Identity en Access Management platform van Conclusion.** Alle ingekochte diensten moeten gekoppeld kunnen worden aan het Conclusion IAM-systeem voor authenticatie en liefst ook autorisatie. *Dit geldt alleen wanneer Conclusion personeel op de dienst moeten inloggen.*		X	X	X

Eisen aan diensten					
#	**Maatregel & Toelichting**	**1**	**2**	**3**	**4**
R-LM-17	**Leverancier hanteert een heldere SLA met servicelevels die overeenkomen met de data classificatie bij Conclusion** Conclusion dient voor zichzelf helder te hebben wat het exact verwacht van de dienstverlening. Hiervoor dient Conclusion zelf de waardeketen te analyseren en te formuleren welke servicelevels wenselijk zijn. Deze servicelevels dienen aan te sluiten op de (standaard) SLA van de dienstverlener. Leverancier dient periodiek te rapporteren aan Conclusion over de actuele/gemeten waarde van deze servicelevels.		X	X	X
R-LM-18	**Leverancier rapporteert over beveiliging** Leverancier rapporteert regulier over eventuele beveiligingsincidenten, kwetsbaarheden en veranderingen in het security landschap en direct over incidenten met een hoog risico voor Conclusion. De betrokken security officer wordt op de hoogte gesteld van deze meldingen.		X	X	X
R-LM-19	**Kritieke kwetsbaarheden worden in de regel direct gecommuniceerd, gemitigeerd en binnen enkele dagen na bekendmaking opgelost** Kritieke lekken die het functioneren van de dienst binnen de Conclusion dienstverlening onmogelijk maakt, worden direct gemitigeerd en zo snel mogelijk opgelost. De exacte termijn moet in de context van de dienst bepaald worden.		X	X	X
R-LM-30	**Leverancier levert een Software Bill of Materials (SBOM) aan, of geeft binnen een dag antwoord op de vraag of een bepaalde software module in gebruik is.** Leverancier dient aan te geven van welke software modules van een derde partij de dienst afhankelijk is. Alternatief mag de leverancier binnen een dag aangeven of er een afhankelijkheid is van een module die op dat moment ter discussie staat.		X	X	X
R-LM-20	**Leverancier geeft volledig inzicht in welke data waar wordt opgeslagen.**	X	X	X	X

Eisen aan diensten					
#	Maatregel & Toelichting	1	2	3	4
	De opslag van data moet transparant zijn, voldoen aan de AVG en passen in de verwerkersovereenkomsten die Conclusion met anderen heeft gesloten				
R-LM-21	**Data mag alleen binnen de EU opgeslagen worden**			X	X
R-LM-22	**Leverancier is transparant over de externe partijen aan wie zij mogelijk klantgegevens moet overhandigen.** Voorbeeld: Amerikaans staatsburgers kunnen verplicht worden mee te werken aan een onderzoek en data te overhandigen. Dit ongeacht de locatie waar de data is opgeslagen. Conclusion wil het risico op dit soort situaties onder controle hebben.		X	X	X
R-LM-23	**Leverancier voldoet aantoonbaar aan Nederlandse en Europese wetten.** Inclusief privacywetgeving.	X	X	X	X
R-LM-24	**Leverancier is bereid bewijsmateriaal beschikbaar te stellen als Conclusion dit rechtswege nodig heeft.** Mocht Conclusion forensisch bewijs nodig hebben in een gerechtelijke context, dan is de leverancier bereid hieraan mee te werken.			X	X
R-LM-25	**Export van de data moet mogelijk zijn.** Bij Cloud services waar data in opgeslagen is moet het mogelijk zijn om de data in een gestructureerd formaat (bv XML) uit de service te halen (liefst automatisch). Dit is voor calamiteit en migratie doeleinden.		X	X	X
R-LM-26	**Het exit scenario dient beschreven te zijn voordat de afname van de dienst begint.** Voordat Conclusion kan beginnen met de afname van de dienst dient het exit scenario beschreven te zijn. In dat exit scenario moet beschreven worden hoe voorkomen kan worden dat de dienstverlening van Conclusion negatief beïnvloed wordt door overstap naar een andere dienstverlener of uitval van de bestaande dienstverlener.			X	X
R-LM-27	**De code en configuratie achter de dienstverlening dient bij een escrow agent gedeponeerd te worden.** Indien de leverancier door onverwachte omstandigheden niet meer in staat is om de dienst te verlenen, moet				X

Eisen aan diensten					
#	**Maatregel & Toelichting**	**1**	**2**	**3**	**4**
	Conclusion eventueel de dienstverlening zelfstandig kunnen voortzetten.				
R-LM-28	**Indien dienst privacygevoelige data doorstuurt of opslaat, is een verwerkersovereenkomst verplicht.** Een verwerkersovereenkomst (of iets dat daar gelijkwaardig aan is) is verplicht bij het doorsturen of opslaan van privacygevoelige data.			X	X

CONCLUSION

CONTACT
Roel Gloudemans (CSO)
security@conclusion.nl