CIO Platform Nederland

CEG Cloud

Essentiële voorwaarden voor een veilig gebruik van Cloud diensten

Checklist

Publicatie van
CEG Cloud & CEG Information Security

CIO Platform Nederland, januari 2015, update december 2016

Van de opstellers

Januari 2015

Alle CIO Interest Groups (CIGs) van het CIOPN hebben het doel om kennis te delen op die terreinen waarvan de leden hebben aangegeven deze belangrijk te vinden.

Dit document bevat een kernachtige beschrijving van essentiële voorwaarden voor een veilig gebruik van cloud diensten. Hiermee een soort 'Checklist' van voorwaarden waaraan wet- en regelgeving en / of gangbare en breed geaccepteerde normen verbonden kunnen worden. Organisatie-specifieke, en dus meer door context ingegeven aspecten, komen niet terug in het overzicht.

Het document is bedoeld als een onderlaag voor en opmaat naar een overeenkomst tussen aanbieder en afnemer, waarin deze aspecten nader worden beschreven en officieel worden bekrachtigd.

Evelijn Jeunink (SURFnet), Jacq de Rijck (Coöperatie VGZ), Andres Steijaert (SURFnet), Edwin Strijland (SVB) en Annemarie Vervoordeldonk (SHV)

December 2016

Binnen de CEG Information Security is een check gedaan op de Cloud Checklist versie januari 2015. Doel is om dit document up-to-date te houden.

Er zijn wijzigingen aangebracht betreffende Safe Harbour en nieuwe ISO-certificeringen zijn opgenomen.

Speciale dank gaat naar Arwin Visser (Royal IHC), Andre Gosens (GVB), Frans van der Boom (CZ), Hein Laan (Rabobank), Jean Paul Dijkstra (TBI), Patrick van de Ven (Royal IHC), Stoffel Bos (Prorail) en Norbert Derickx (CIO Platform Nederland).

Inhoudsopgave

Toepasbaarheid Checklist

1.1. Individueel

Leden van het CIO Platform Nederland kunnen het overzicht gebruiken:

- Als start- en referentiepunt bij leverancierscontacten;
- Bij het inkopen van cloud diensten, door de beschrijving als houvast te gebruiken om goede gebruiksvoorwaarden vast te leggen.

1.2. Gezamenlijk

Door als community van afnemers, verenigd in CIO Platform Nederland, allen deze set van basisvoorwaarden te hanteren, ontstaan:

- een brede basis;
- en gemeenschappelijke taal;

waarmee een grootschaliger gebruik van cloud diensten, tegen de juiste voorwaarden, tot stand kan komen.

Het document is een aanvulling op andere (binnen de CIG Cloud van het CIO Platform Nederland geproduceerde) cloud documenten, waaronder de cloud checklist.

Opzet Checklist

In de beschrijving van essentiële voorwaarden voor een veilig gebruik van cloud diensten staan bedrijfsbelang en risico-inschatting centraal, bij het invullen van zes aandachtsgebieden:

A. (Intellectueel) eigendom, eigenaarschap en zeggenschap

B. Wet- en regelgeving (met speciale aandacht voor het onderdeel privacy)

C. Beveiliging en data integriteit

D. Kwaliteit en continuïteit

E. Vertrouwelijkheid

F. Toezicht en meldingsplicht

Voor alle elementen in de beschrijving geldt dat deze:

- contractueel dienen te worden vastgelegd, in een schriftelijke overeenkomst tussen Aanbieder en Afnemer;
- van toepassing zijn op Aanbieder, alsmede onderaannemers (derden) die Aanbieder inschakelt bij werkzaamheden. Aanbieder is verantwoordelijk voor deze onderaannemers.

A. (Intellectueel) eigendom, eigenaarschap en zeggenschap

1) Alle (intellectuele) eigendomsrechten op (het bestand c.q. de bestanden van) de gegevens blijven te allen tijde berusten bij de Afnemer.

2) Aanbieder heeft geen zelfstandige zeggenschap over de gegevens die door haar worden verwerkt. De zeggenschap over de gegevens berust bij Afnemer.

B. Wet en regelgeving

1) De Afnemer is Verantwoordelijk en de Aanbieder heeft de rol van Bewerker.

2) Voor data export (doorgifte van persoonsgegevens) / internationale uitwisseling wordt geborgd dat data enkel wordt uitgewisseld met landen en bedrijven die beschikken over een passend beschermingsniveau. Aanbieder en Afnemer stellen hiertoe het beschermingsniveau van het land van Aanbieder vast en afhankelijk van het daar aanwezige beschermingsniveau worden waar nodig extra afspraken gemaakt over toezicht en naleving.

a. Voor landen in de EU of op de Europese witte lijst is de privacy gewaarborgd via wet- en regelgeving en zijn geen extra afspraken tussen Aanbieder en Afnemer vereist.
b. Indien het land zich niet in de EU bevindt of niet op de Europese witte lijst, is geen passend beschermingsniveau aanwezig. Het is dan nodig afspraken te maken via een Europees modelcontract, Vergunning (vangnet-bepaling) of door de betreffende Data Protection Authorities goedgekeurde Binding Corporate Rules, die omschrijven hoe een bedrijf omgaat met de verwerking van persoonsgegevens.

3) Er is mogelijk sprake van andere geldende wet- en regelgeving, waaronder de archiefwet, fiscale wet- en regelgeving, exportregels en eDiscovery.

C. Beveiliging en data integriteit

1) Aanbieder treft passende maatregelen om de fysieke en logische beveiliging van de Clouddienst adequaat in te richten tegen verlies of aantasting en tegen enige vorm van onbevoegde kennisneming, wijziging en verstrekking dan wel anderszins onrechtmatige verwerking van de gegevens.

2) Indien gevoelig materiaal: ISO27001 (of afgeleiden, zoals: **BIR en** NEN7510), ISO27015.

3) Indien privacy gevoelig: ISO 27018.

D. Kwaliteit en continuïteit

1) Aanbieder is verantwoordelijk voor de kwaliteitsaspecten van de Clouddienst en het dienstniveau van de Clouddienst, conform gemaakte afspraken:

a. Aanbieder heeft een escalatie- en communicatieplan;
b. Aanbieder biedt een ondersteuningsclausule, met daarin opgenomen een prioritering bij calamiteiten;
c. Aanbieder en Afnemer maken afspraken over de beschikbaarheid van de Clouddienst.

2) Aanbieder en Afnemer komen een Exit strategie overeen (bij beëindiging dienst of faillissement Aanbieder), waarin tenminste de volgende aspecten worden benoemd:

a. rollen, taken en verantwoordelijkheden;
b. de condities waaronder de exit strategie in werking treedt;
c. data portabiliteit:
    i. de wijze waarop het mogelijk is om data te onttrekken;
    ii. de wijze waarop data overgebracht kan worden naar een andere Aanbieder;
d. de wijze waarop data vernietigd kan worden / wordt.

3) Aanbieder draagt zorg voor adequate 'disaster recovery' voorzieningen om beschikbaarheid van de Clouddienst, en daarmee van de gegevens, te waarborgen.

4) Aanbieder biedt inzicht in en inspraak bij de verander- (wat) en release kalender (wanneer) van de Clouddienst.

5) Aanbieder en Afnemer leggen de in de Clouddienst gehanteerde uitwisselingsstandaarden vast, inclusief de ondersteuningsperiode van deze uitwisselingsstandaarden.

E. Vertrouwelijkheid

1) Aanbieder houdt vertrouwelijke gegevens geheim. Dit betekent tenminste dat:

a. Alle gegevens vertrouwelijk zijn (waaronder wordt verstaan: mogen niet openbaar gemaakt worden), tenzij anders aangegeven;
b. Aanbieder zal voor haar werkzame personen (waaronder werknemers) die betrokken zijn bij de verwerking van vertrouwelijke gegevens, contractueel verplichten tot geheimhouding van die vertrouwelijke gegevens;
c. Aanbieder en Afnemer leggen de gevolgen van schending van de vertrouwelijkheid vast.

F. Toezicht en meldingsplicht

1) Aanbieder verleent op eerste verzoek van Afnemer haar medewerking aan het uitoefenen van toezicht door of namens de Afnemer op de bewaring en het gebruik van gegevens door Aanbieder.

2) Aanbieder stelt alle gegevens die zij in het kader van de uitvoering van de Overeenkomst onder zich heeft, inclusief eventueel daarvan gemaakte kopieën, op eerste verzoek aan Afnemer ter beschikking.

3) Aanbieder informeert Afnemer onmiddellijk nadat zij bekend is geworden met een vermoedelijk(e) of daadwerkelijk(e):

i. degradatie van de kwaliteit (waaronder 'onbeschikbaarheid');
ii. schending van de geheimhoudingsplicht;
iii. verlies, diefstal of misbruik van vertrouwelijke en/of persoonsgegevens; dan wel of
iv. schending van de beveiligingsmaatregelen;

dan wel de verwachting heeft dat één van deze zaken gaat optreden.

Mede opdat de Afnemer kan voldoen aan de brede meldplicht, die onderdeel is van het wetsvoorstel datalekken dat nu bij de Tweede Kamer ligt.

4) Afnemer is in staat periodiek een audit uit te (laten) voeren, om zo te toetsen of Aanbieder handelt conform afspraken en geldende wet- en regelgeving.

5) Afnemer heeft het recht om vanuit gebruikersperspectief de kwaliteitsaspecten en het dienstniveau van de Clouddienst te controleren en wordt hier door Aanbieder niet in beperkt.

6) Aanbieder spant zich maximaal in om de belangen van Afnemer te behartigen bij inzageverzoeken en / of -bevelen van autoriteiten door:

a. te toetsen of er een wettelijke verplichting is om in te gaan op het verzoek / bevel;
b. bezwaar te maken tegen het verzoek / bevel waar mogelijk;
c. niet meer gegevens te verstrekken dan nodig (enkel een minimale gegevensset);
d. en de Afnemer te informeren zodra mogelijk.