

Gedragcode leden Dutch Cloud Community

GEDRAGSCODE VOOR LEDEN VAN DE DUTCH CLOUD COMMUNITY

Versie 1.0 gepubliceerd op 1 maart 2021.

Versie 2.0 gepubliceerd op 15 mei 2024.

Versie 3.0 gepubliceerd op 11 oktober 2024.

De DCC Gedragcode is geborgd in de statuten van de Vereniging Dutch Cloud Community onder artikel 6 lid 2b.

Deze Gedragcode geeft de verplichtingen van redelijk, aanvaardbaar en compliant gedrag voor de Leden van de Dutch Cloud Community (DCC) met betrekking tot hun gedrag als dienstverlener naar hun markt-relaties, mede-deelnemers, personeel, autoriteiten en de maatschappij als geheel.

Deze DCC Gedragcode zal regelmatig worden getoetst en waar nodig aangepast op initiatief van DCC rekening houdende met ontwikkelingen in wet- en regelgeving.

In geval van wijzigingen zal DCC dit op haar website bekend maken en publiceren aan haar Leden. Binnen 14 dagen na publicatie van de aangepaste DCC Gedragcode op de website van DCC wordt deze automatisch van kracht voor alle DCC Leden.

Deze Gedragcode bestaat uit drie delen:

- A. De verplichtingen van Leden waarin algemene- en maatschappelijke verantwoordelijkheid uiteengezet wordt.
- B. De verplichtingen van Leden om dienstverlening op een professionele, betrouwbare en verantwoordelijke wijze uit te voeren;
- C. De verplichtingen van Leden om de sector brede "[Gedragcode Abusebestrijding](#)" inclusief KYC verplichtingen en de gedragscode "[Responsible disclosure](#)" zorgvuldig na te leven.

A. Algemene- en Maatschappelijke Verantwoordelijkheid

1. DCC leden accepteren deze DCC Gedragcode en voeren hun activiteiten uit op basis van deze DCC Gedragcode met inachtneming van integriteit, openheid, eerlijkheid en met respect voor de belangen van andere marktpartijen, medewerkers, de branche en de maatschappij.
2. DCC Leden erkennen hun maatschappelijke verantwoordelijkheid met betrekking tot het borgen van betrouwbaarheid en veiligheid van hun dienstverlening.
3. DCC Leden erkennen hun maatschappelijke verantwoordelijkheid met betrekking tot duurzaamheid waaronder groen energiegebruik, en borging van diensten en datacenters die voldoen aan eisen van zelfregulering, wet- en regelgeving op het gebied van milieu en energie, bijvoorbeeld de milieunormen van de ISO14001.

4. DCC Leden voeren beleid voor continue verbetering van kennis en vaardigheden van hun medewerkers door opleidingen en certificeringen.
5. DCC Leden zullen zich ervan onthouden publieke uitlatingen te doen die op onredelijke wijze afbreuk doen aan de reputatie van DCC, van andere Leden of de cloud sector.
6. DCC Leden maken hun lidmaatschap van de vereniging Dutch Cloud Community en hun conformiteit aan deze DCC Gedragscode kenbaar op hun bedrijfswebsite.

B. Dienstverlening

7. DCC Leden bieden diensten aan op professionele wijze waarbij de organisatie onderdelen voldoende gekwalificeerd zijn.
8. DCC Leden kunnen bepaalde diensten leveren op basis van een redelijke Service Level Agreement (SLA) waarin definities en onderwerpen zijn opgenomen zoals onder meer genoemd in het Framework SLA van de Dutch Cloud Community.
9. DCC Leden verplichten zich tot het nastreven van optimale beschikbaarheid en continuïteit van hun dienstverlening, en het adequaat beveiligen van diensten, informatie, toegang en netwerken, bijvoorbeeld door certificering van ISO 27001.
10. DCC Leden hanteren de bepalingen van de EU privacy wetgeving (GDPR, AVG) en hanteren de daarbij gebruikelijke documenten zoals verwerkersovereenkomst (ex. art. 28 lid 3 AVG), met verwijzing naar de geldende EU Standard Contractual Clauses, Adequacy Decisions en/of EU US Privacy Framework in geval van overdracht van persoonsgegevens buiten de EU.
11. DCC Leden streven naar zoveel mogelijk cloud computing infrastructuur en opslag met gebruikmaking van datacenters in- en onder de jurisdictie van de EU alsmede het behoud van management, uitvoering en control voor eindverantwoordelijkheid van data en security onder (alleen) EU wetgeving.
12. DCC Leden borgen redelijke migratie mogelijkheden. Waaronder redelijke kosten en redelijke voorwaarden voor migratie voor de klant Voor migratie naar andere dienstverleners met inachtneming van wet- en regelgeving zoals de Data Act voor cloud service providers, waaronder EU model contracten die beschikbaar zullen zijn. En zien toe klant migratie mogelijk is op basis van redelijke contractuele rechten en verplichtingen conform wet- en regelgeving.
13. DCC Leden streven ernaar om hun klanten de mogelijkheid te bieden voor beschermingsregelingen tegen risico's die de continuïteit van de dienst bedreigen op redelijke voorwaarden door het aanbieden van bijvoorbeeld migratieregelingen, of collectieve voorzieningen bij voorbaat vastgelegd met derden-dienstverleners, tegen een redelijke vergoeding.
14. DCC Leden treffen redelijke voorzieningen ter bescherming van hun eigen bedrijfscontinuïteit en tegen de eventuele gevolgen van financiële risico's door

bijvoorbeeld claims en rechtszaken, onder andere zoals door middel van het afsluiten van een beroepsaansprakelijkheidsverzekering.

15. DCC Leden verplichten zich tot het zorgvuldig naleven en omgaan met intellectuele eigendomsrechten waaronder het correct toepassen en respecteren van licentie- en gebruiksvoorwaarden van hun toeleveranciers.

C. KYC en Bestrijding van Illegale online Inhoud

(conform Digital Services Act – Abuse-bestrijding)

16. DCC Leden verplichten zich tot het opvolgen van de toepasselijke wet- en regelgeving waaronder de Digital Services Act (Digitale Diensten Verordening voor het bestrijden van Illegale online Inhoud) door het implementeren en handhaven van deze verplichtingen in de eigen gedragscodes van het DCC Lid op basis van cq conform de "[Gedragscode Illegale Inhoud \(Abuse\) bestrijding](#)" en vermelden dit op hun DCC Lid bedrijfswebsite. Op de website van de Autoriteit Consument en Markt worden hiertoe ook overzichtelijke aanwijzingen gegeven in de ACM documenten: DSA Leidraad met zorgvuldigheidsverplichtingen Digitale Diensten.

Deze DSA Bestrijding van Online Illegale Inhoud Gedragscode bevat de volgende elementen:

1. Beleid: Operators van digitale infrastructuur (= tussenhandeldiensten conform de DSA):
 1. Zijn in beginsel niet aansprakelijk noch verantwoordelijk voor de activiteiten van de afnemers van hun diensten. Dat neemt niet weg dat zij al wat in hun mogelijkheden ligt zullen doen om Abuse te bestrijden.
 2. Hanteren daartoe deze Gedragscode, zullen dat duidelijk kenbaar maken op hun site c.q. communiceren daarover naar hun afnemers en medewerkers.
 3. Hanteren een Acceptable Use Policy voor hun afnemers en/of gebruikers, waarin wordt vastgelegd wat van hen wordt verwacht indien Abuse bij hun activiteiten van afnemers wordt aangetoond.
 4. Hanteren de gedragscode Notice en Take Down / Notice en Stay Down en implementeren de bijbehorende processen in hun organisatie.
 5. Hanteren (een) industry best practice(s) voor Abuse bestrijding die past bij hun cloud service provider activiteiten, zoals de gedragscode van de [M3AAWG](#) voor [cloud/hosting providers](#) en maken dit (deze) kenbaar naar hun afnemers.
 6. Doen al wat redelijkerwijs binnen hun mogelijkheden ligt om de effecten van Abuse binnen hun netwerken te verminderen voor andere gebruikers van het

internet. Autonomous Systems doen dat door in ieder geval het toepassen van de maatregelen beschreven in MANRS (<https://www.manrs.org/>).

7. Voeren beleid om hun performance op het gebied van het bestrijden van Online Illegale Inhoud, dus zoals voorheen Abuse bestrijding continu te verbeteren.
8. Voeren beleid om in Know Your Customer eisen deugdelijk en effectief toe te passen. Dat wil zeggen: Weten wie hun afnemers zijn, en dat hun afnemers in deugdelijke segment de cloud diensten gebruiken, en doen al wat redelijkerwijs binnen hun mogelijkheden ligt om zich ervan te verzekeren dat zij altijd kunnen weten wie de eindverantwoordelijke is voor de accounts van hun afnemers cq klanten.

2. Know your customer Beleid: Operators van digitale infrastructuur (= tussenhandeldiensten conform de DSA):

1. Nemen stappen om te voorkomen dat hun gebruikers en afnemers van hun diensten cq klanten anoniem en niet traceerbaar zijn.
2. Nemen verificatie stappen om te borgen dat wanneer een nieuwe klant zich aanmeldt, ook indien de klant met crypto-currencies wil betalen, moet er voor de eerste betaling een succesvolle verificatie stap hebben plaatsgevonden.
3. Nemen stappen voor verificatiemogelijkheden onder andere, maar niet beperkt tot:
 - Persoonsgegevens
 - Bankgegevens (eenmalige overmaking van 1 cent)
 - KvK-gegevens
 - UBO
 - Legal Entity Identifier
 - Authenticatie legitimatiebewijs

3. Informatie: Operators van digitale infrastructuur (= tussenhandeldiensten conform de DSA):

1. Publiceren op hun website en in de ter zake doende whois registraties contactgegevens voor het melden van illegale inhoud online, dus Abuse volgens de eisen van de geldende regelgeving.
2. Doen al wat redelijkerwijs binnen hun mogelijkheden ligt om informatie te verkrijgen over kwetsbaarheden en abuse in hun netwerken en op hun voorzieningen. Dat doen zij door zich in ieder geval te abonneren op abuse feeds, of zich aan te sluiten bij [CleanNetworks](#) of het raadplegen van/aansluiten bij andere informatiebronnen die daarover inzicht geven.

3. Accepteren in redelijkheid alle Abuse meldingen die ze ontvangen via geautomatiseerde systemen en door personen opgestelde individuele meldingen.
 4. Stellen zich op de hoogte van hun performance op het gebied van Abuse bestrijding door raadplegen van de daartoe beschikbare bronnen.
4. Meldingen: Operators van digitale infrastructuur (= tussenhandeldiensten conform de DSA):
1. Zorgen voor correcte contactgegevens van hun klanten, gebruikers- en/of afnemers zodat bij Abuse of het vermoeden ervan er direct contact gelegd kan worden met de afnemer.
 2. Zijn proactief naar hun klanten, afnemers of gebruikers; dat wil zeggen ze nemen actie als zij in kennis worden gesteld van Abuse of kwetsbaarheden in hun diensten.
 3. Zullen bij die vormen van abuse waarbij de operator kennis heeft genomen van de aard van het Abuse en het voortduren ervan ernstige schade aan individuen oplevert, direct maatregelen nemen om verdere schade te voorkomen of te beperken. CSAM, phishing, hacking, malafide webshops en mal-ware verspreiding worden in ieder geval geschaard onder deze vormen van Abuse.
 4. Verplichten zich om bij langdurig, substantieel of herhaald overtreden van de acceptable use policy door hun afnemers de dienstverlening te schorsen, diensten in quarantaine te plaatsen of de contracten met zulke klanten te beëindigen.

Niet nakoming aan bovenstaande Verplichtingen

17. Indien de Dutch Cloud Community constateert -of erop wordt gewezen – of dat er redelijkerwijs aanleiding is dat een DCC Lid een verplichting van deze DCC Gedrags Code niet nakomt dan zal de Dutch Cloud Community een nieuw onderzoek starten naar het (mogelijk) niet nakomen door het DCC Lid van de verplichtingen in deze DCC Gedragscode. Indien na dergelijk onderzoek redelijkerwijs kan worden vastgesteld dat het DCC Lid de verplichtingen van de DCC Gedragscode niet nakomt zal het DCC bestuur het betreffende DCC Lid schriftelijk wijzen op deze verplichting tot nakoming, en het DCC Lid in gebreke stellen om de verplichtingen van de DCC Gedragscode binnen aan te geven redelijke termijn alsnog na te komen.

18. Indien het DCC Lid de verplichting(en) van de DCC Gedragscode blijvend niet nakomt en niet herstelt binnen de aangegeven redelijke termijn, zal het Dutch Cloud Community bestuur op basis van statutaire bepalingen overgaan tot maatregelen waartoe het bestuur bevoegd is waaronder schorsing, opzegging, ontzetting (royement) danwel andere besluiten van het DCC bestuur bijvoorbeeld het opleggen

tot verwijdering van het Dutch Cloud Community logo op de website van het DCC Lid en verwijdering van het logo van het DCC Lid op de website van DCC conform de daartoe bestaande wettelijke-, contractuele en statutaire mogelijkheden.

De branche waar de Dutch Cloud Community actief is verandert snel. Deze Gedragscode zal dan ook periodiek worden herzien door het bestuur van DCC.