Gedragscode Abusebestrijding 2024

Versie 2.0 – oktober 2024

De samenleving moet erop kunnen vertrouwen dat aanbieders van digitale infrastructuur zich inspannen om gebruik van hun faciliteiten voor onrechtmatige activiteiten waaronder maar niet beperkt tot illegale inhoud te voorkomen en te verspreiden. Daartoe hanteren zulke aanbieders deze Gedragscode Abusebestrijding (“Gedragscode”).

Voor de toepassing van deze Gedragscode wordt verstaan onder:

- **Aanbieder**: een natuurlijke of rechtspersoon die digitale infrastructuur aanbiedt of beheert.
- **Digitale infrastructuur**: op internet aangesloten faciliteiten die digitale online-diensten faciliteren, in brede zin, waaronder datacenters, hosting- en cloudplatforms, domeinen, netwerken (AS), internet access; en al datgene wat als een mere-conduit activiteit en hosting wordt beschouwd en eveneens op die wijze onder de DSA als zodanig is gedefinieerd.
- **Abuse**: het misbruik van op internet aangesloten digitale infrastructuur in brede zin; zoals het versturen van spam of phishing e-mails, het verspreiden van malware, DDoS, runnen van een botnet, runnen van een frauduleuze website, opslaan en verspreiden van CSAM, terroristische inhoud of andere illegale inhoud of informatie die illegaal is omdat zij verband houdt met illegale inhoud, producten, diensten of activiteiten, et cetera (hierna “Abuse”). Abuse omvat in elk geval onmiskenbaar onrechtmatige activiteiten en voorts datgene wat door de betreffende Aanbieder als ongewenst wordt beschouwd.

Beleid

- Aanbieders 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.
- Aanbieders hanteren daartoe deze Gedragscode, zullen dat duidelijk kenbaar maken op hun site c.q. communiceren daarover naar hun afnemers en medewerkers.
- Aanbieders hanteren een Abuse Policy voor hun afnemers en/of gebruikers van diensten, waarin wordt vastgelegd wat van hen wordt verwacht indien Abuse bij hun activiteiten wordt aangetoond.
- Aanbieders hanteren een Acceptable Use Policy voor hun afnemers en/of gebruikers van diensten, waarin wordt vastgelegd op welke wijze of voor welke doeleinden hun diensten gebruikt mogen worden.
- Aanbieders hanteren de Gedragscode Notice and Take Down en implementeren de bijbehorende processen in hun organisatie.
- Aanbieders ondernemen daadwerkelijke actie indien een formeel bevel wordt ontvangen tot het nemen van actie met betrekking tot illegale inhoud van daartoe bevoegde instanties, koppelen terug wat ze hebben ondernomen aan deze instanties en verschaffen informatie over individuele ontvangers van de dienst indien zij een vordering ontvangen.

- Aanbieders hanteren (een) industry best practice(s) voor Abusebestrijding die past bij activiteiten en hun diensten en rol onder de DSA, zoals de gedragscode van de M3AAWG voor cloud/hosting providers en maken dit (deze) online kenbaar naar hun afnemers.
- Aanbieders doen al wat redelijkerwijs binnen hun mogelijkheden ligt om de effecten van Abuse binnen hun netwerken en afnemers van hun diensten te verminderen voor andere gebruikers van het internet. Autonomous Systems doen dat door in ieder geval het toepassen van de maatregelen beschreven in MANRS.
- Aanbieders voeren beleid om hun performance op het gebied van Abusebestrijding continue te verbeteren.
- Aanbieders voeren beleid om Know Your Customer deugdelijk en effectief toe te passen. Dat wil zeggen: weten wie hun afnemers zijn en waar en hoe deze te betrekken zijn in de bestrijding van Abuse, en doen al wat redelijkerwijs binnen hun mogelijkheden ligt om zich ervan te verzekeren dat zij altijd weten wie de verantwoordelijke is voor de accounts van hun afnemers.

Know Your Customer Beleid

- Aanbieders nemen maatregelen om te voorkomen dat afnemers van hun diensten niet identificeerbaar zijn.
- Aanbieders nemen verificatiemaatregelen om te borgen dat wanneer een nieuwe afnemer zich aanmeldt, ook indien de afnemer met cryptovaluta wil betalen, er voor de eerste betaling een succesvolle verificatieprocedure heeft plaatsgevonden.
- Aanbieders nemen maatregelen voor verificatiemogelijkheden zoals bijvoorbeeld, maar niet beperkt tot:
    - Persoonsgegevens
    - Bankgegevens (eenmalige overmaking van 1 cent)
    - KvK-gegevens
    - Ultimate Beneficial Ownership (UBO)
    - Legal Entity Identifier (LEI)
    - Authenticatie legitimatiebewijs

Informatie

- Aanbieders publiceren op hun website en in de ter zake doende “whois-registraties” contactgegevens voor het melden van Abuse volgens de eisen van de geldende regelgeving.
- Aanbieders 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 Clean Networks of het raadplegen van/aansluiten bij andere informatiebronnen die daarover inzicht geven.
- Aanbieders accepteren in redelijkheid alle Abusemeldingen die ze ontvangen via geautomatiseerde systemen en door personen opgestelde individuele meldingen.

- Aanbieders stellen zich op de hoogte van hun performance op het gebied van Abusebestrijding door het raadplegen van daartoe beschikbare bronnen.

Meldingen

- Aanbieders zorgen voor correcte contactgegevens van hun afnemers zodat bij Abuse of het vermoeden ervan er direct contact gelegd kan worden met de afnemer.
- Aanbieders zijn proactief naar afnemers; dat wil zeggen ze nemen actie als zij in kennis worden gesteld van Abuse in hun diensten.
- Aanbieders zullen bij die vormen van Abuse waarbij de Aanbieder 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.
- Aanbieders 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 afnemers te beëindigen.

Niet-nakoming

- Aanbieders, en daarmee gebruikers van deze Gedragscode kunnen het redelijke vermoeden van niet-nakoming van deze Gedragscode melden aan (een van de) organisaties die deze Gedragscode vertegenwoordigen.
- Deelnemers aan deze Gedragscode zullen zich indien mogelijk onthouden van zakelijke relaties met organisaties waarvan bekend is dat ze evident handelen in strijd met deze Gedragscode, c.q. waarvan in redelijkheid kan worden gesteld dat ze onrechtmatigheden opzettelijk faciliteren.

Herziening en beheer

Deze Gedragscode Abusebestrijding zal jaarlijks worden herzien, op basis van regelgeving, feedback en ervaringen van de deelnemers aan deze Gedragscode. Bij elke herziening zal het versienummer worden bijgewerkt en zullen de wijzigingen worden gedocumenteerd in de revisiegeschiedenis. De NBIP is beheerder van deze Gedragscode en verantwoordelijk voor het versiebeheer.

Vertegenwoordigers Gedragscode

De volgende organisaties hebben actief bijgedragen aan het opstellen van deze Gedragscode:

- Stichting Digitale Infrastructuur Nederland (DINL)
- Dutch Cloud Community (DCC)
- Nationale Beheersorganisatie Internet Providers (NBIP)
- Vereniging van Registrars (VvR)

Onderschrijvers Gedragscode

De volgende organisaties onderschrijven de principes en doelstellingen van deze Gedragscode Abusebestrijding en committeren zich aan het uitdragen en naleven van deze standaarden:

- Dutch Data Center Association (DDA)
- Anti Abuse Netwerk (AAN)

Revisiegeschiedenis

Versie 2.0 - Oktober 2024

- Uitgebreide herziening van de gehele Gedragscode
- Toevoeging van nieuwe secties: Know Your Customer Beleid, Niet-nakoming en Onderschrijvers Gedragscode
- Aanpassing van definities en beleid om aan te sluiten bij recente ontwikkelingen en regelgeving

Versie 1.0 - November 2021

- Initiële publicatie van de Gedragscode