Fox-IT: "For A More Secure Society"

In dit beleid wordt de manier beschreven waarop Fox-IT invulling geeft aan maatschappelijk verantwoord ondernemen (MVO). Voor ons betekent MVO de verantwoordelijkheid die wij dragen voor de effecten van onze activiteiten op de maatschappij, waarbij de borging van mensenrechten centraal staat. Wij willen bijdragen aan een veiligere samenleving en hebben integriteit en vertrouwelijkheid hoog in het vaandel staan.

Het is nodig om bepaalde activiteiten geheim te houden, gezien het belang van onze klanten en de gevoelige aard van onze werkzaamheden. Met het navolgende MVO beleid geven wij daarom meer in het algemeen inzicht in onze uitgangspunten, de wijze waarop wij omgaan met dilemma's rond maatschappelijk relevante vraagstukken en het toetsingskader dat wij hanteren met betrekking tot (potentiële) klanten.

1. Uitgangspunten

De OESO Richtlijnen voor Multinationale Ondernemingen vormen de basis van ons MVO beleid. Dit zijn MVO-normen voor internationaal ondernemen.[1] Ze maken duidelijk wat van internationaal opererende bedrijven wordt verwacht op het gebied van MVO. De OESO-richtlijnen worden onderschreven door de nationale overheden van meer dan 40 landen, waaronder de Nederlandse overheid. Alle hoofdstukken van de OESO-richtlijnen zijn relevant, maar we besteden in het bijzonder aandacht aan:

Mensenrechten

Fox-IT respecteert de mensenrechten zoals die beschreven staan in het Europees Verdrag voor de Rechten van de Mens.[2] De producten en diensten van Fox-IT zijn er primair op gericht om de samenleving veiliger te maken, waardoor inbreuken op mensenrechten voorkomen kunnen worden. Fox-IT helpt verder om inbreuken op mensenrechten door derden te verhinderen. Ongunstige effecten op mensenrechten die direct verband houden met onze bedrijfsactiviteiten of die van onze partners proberen we altijd te voorkomen. Als deze ongunstige effecten zich onverhoopt toch voordoen, treffen we passende maatregelen om ze zoveel mogelijk te beëindigen of beperken. Voor projecten en ontwikkelingen waarbij mensenrechten in het geding zouden kunnen zijn, voeren we risicoanalyses uit (*due diligence*).[3]

---

[1] Ministerie van Buitenlandse Zaken, *De OESO-richtlijnen voor Multinationale Ondernemingen, Aanbevelingen voor verantwoord ondernemen in een mondiale context* (Den Haag: Nederlandse vertaling, 2011) <http://www.oesorichtlijnen.nl/oeso-richtlijnen/download-de-oeso-richtlijnen>.

[2] Mensenrechten zijn fundamentele rechten die ieder mens toekomen, waar ook ter wereld. Mensenrechten beschermen burgers tegen de macht van de staat en moeten ervoor zorgen dat iedereen kan leven in menselijke waardigheid. Mensenrechten zijn inherent, onvervreemdbaar, universeel, ondeelbaar en onderling afhankelijk. Raad van Europa, *Verdrag 4 november 1950 tot bescherming van de rechten van de mens en de fundamentale vrijheden* <http://www.echr.coe.int/Documents/Convention_NLD.pdf>.

[3] Onder *due diligence* verstaan we het uitvoeren van een risicoanalyse. Het doel is om de risico's op de mogelijke inbreuk op mensenrechten in kaart te brengen en deze te voorkomen of te verminderen.

Wetenschap & technologie
Fox-IT draagt bij aan de ontwikkeling van kennis op technologisch en wetenschappelijk gebied. Bij de totstandkoming van onze producten houden we rekening met de kansen maar ook met de risico's op het gebied van MVO. Wij hanteren een werkwijze die de overdracht en snelle verspreiding van technologie en kennis mogelijk maken. Indien wij licenties voor het gebruik van intellectuele eigendomsrechten verlenen of op een andere manier technologie ter beschikking stellen, doen we dit onder redelijke voorwaarden en bepalingen. We zetten gezamenlijke onderzoeks- en innovatieprojecten op met onderzoeksinstellingen, universiteiten, bedrijven en andere organisaties.

Onze producten en diensten zijn gericht op het voorkomen en mitigeren van beveiligingsrisico's. Bij de ontwikkeling van nieuwe producten en diensten van Fox-IT wordt ook de potentie voor misbruik daarvan onderzocht en zo goed mogelijk voorkomen. De ontwikkeling van nieuwe technologieën leidt ook tot bredere maatschappelijke uitdagingen. Fox-IT zet zich in voor een veiligere samenleving, bijvoorbeeld door onderzoek te doen naar en ruchtbaarheid te geven aan dreigingen op het internet. Wij gaan het debat aan over technologische ontwikkelingen en vragen aandacht voor de risico's die deze ontwikkelingen met zich meebrengen.

Fox-IT spant zich ook in om maatschappelijk relevante partijen te ondersteunen. Als maatschappelijk relevante partijen onze producten of diensten niet kunnen bekostigen leveren wij onze producten of diensten desgevraagd soms zonder daarvoor kosten in rekening te brengen.

2. MVO gedragscode

Deze code bevat de gedragsregels die iedereen bij Fox-IT dient na te leven. De code ondersteunt onze wijze van ondernemingsbestuur. De gedragscode treedt in werking op 1 november 2014.

Gedragsnormen
Wij voeren onze activiteiten uit op basis van eerlijkheid en integriteit, met respect voor mensenrechten en de belangen van onze medewerkers. Wij respecteren de rechtmatige belangen van alle partijen op wie onze activiteiten betrekking hebben.

Naleving van de wet
Fox-IT en zijn medewerkers dienen zich aan de relevante wetten te houden van de landen waarin wij opereren. Als in het kader van de lokale wetgeving bepaalde handelingen toelaatbaar zijn die strijdig zijn met Fox-IT's beleid voor Maatschappelijk Verantwoord Ondernemen, dan zullen wij deze niet uitvoeren.

Medewerkers
Fox-IT streeft naar verscheidenheid onder zijn medewerkers, in een werkomgeving waar mensen elkaar met vertrouwen en respect bejegenen en waar iedereen zich verantwoordelijk voelt voor de resultaten en de reputatie van ons bedrijf. Wij willen samen met onze

medewerkers de vaardigheden en capaciteiten van ieder van hen ontwikkelen en vergroten. Wij respecteren de waardigheid van het individu en het recht van medewerkers op vrijheid van vereniging. We zorgen voor een goede communicatie met onze medewerkers door middel van informatie- en overlegprocedures. Onze kernwaarden en uitgangspunten staan uitgebreid beschreven in het Fox-IT Manifest.

Zakenpartners

De relaties van Fox-IT met leveranciers, afnemers en zakenpartners strekken tot wederzijds voordeel. In onze zakelijke contacten verwachten wij van zakenpartners dat zij gedragsregels hebben die lijken op de onze. Als dergelijke regels ontbreken, moedigen we zakenpartners aan om ze op te stellen. Bij het uitblijven daarvan, of wanneer in strijd wordt gehandeld met het MVO beleid van Fox-IT, dan kan de directie daar consequenties aan verbinden, zoals het beëindigen van de relatie.

Maatschappelijke activiteiten

Fox-IT heeft een unieke kennispositie en kent de nieuwste technologische ontwikkelingen. Wij stimuleren onze medewerkers om deel te nemen aan het maatschappelijk debat en geven gevraagd en ongevraagd advies over voorgenomen wet- en regelgeving. Wij zijn transparant over deze inhoudelijke bijdragen. Fox-IT ondersteunt geen politieke partijen en verstrekt geen financiële middelen ter bevordering van politieke doeleinden. Fox-IT nodigt andere bedrijven uit om mee te denken over de toekomst van de cybersecurity sector.

Mededinging

Fox-IT gelooft in krachtige en eerlijke mededinging en ondersteunt de ontwikkeling van passende wetgeving op dit gebied. Fox-IT handelt in overeenstemming met de principes van eerlijke mededinging en met alle geldende voorschriften.

Zakelijke integriteit

Fox-IT geeft noch ontvangt steekpenningen of andere oneigenlijke voordelen gericht op zakelijk of financieel gewin. Het is geen enkele medewerker toegestaan een gift of betaling aan te bieden, te geven of te ontvangen die smeergeld vertegenwoordigt of als zodanig moet worden geïnterpreteerd. Ieder verzoek om of aanbod van smeergeld dat verband houdt met (mogelijke) werkzaamheden van Fox-IT moet onmiddellijk worden afgewezen en wetenschap daarvan moet aan de ethische commissie en de directie worden gerapporteerd. Bij twijfel kunnen medewerkers de situatie voorleggen aan de ethische commissie. Fox-IT's financiële administratie en ondersteunende documenten omschrijven de aard van de onderliggende transacties nauwkeurig. Geheime of niet-geregistreerde rekeningen, geldbedragen of activa worden niet gecreëerd.

Belangen

Ondernemerschap van medewerkers van Fox-IT binnen en buiten het bedrijf wordt aangemoedigd. Van alle medewerkers wordt echter verwacht dat zij persoonlijke activiteiten en financiële belangen die strijdig zouden kunnen zijn met hun verantwoordelijkheden bij

Fox-IT of het maatschappelijk belang vermijden. Het is medewerkers verboden gewin voor zichzelf of anderen na te streven door misbruik te maken van hun positie.

Naleving

Naleving van deze gedragscode is belangrijk voor de toekomst van Fox-IT. De directie is ervoor verantwoordelijk dat deze gedragsregels overal binnen het bedrijf worden doorgevoerd en nageleefd. Om uitvoering te geven aan deze verantwoordelijkheid steltde directie een onafhankelijke ethische adviescommissie aan. In de ethische commissie worden ethische, juridische en technische kennis verenigd. De ethische commissie stelt procedures en gedragsregels vast die voortvloeien uit het MVO beleid en ziet toe op de naleving daarvan, voert risicoanalyses uit in het kader van due dilligence, adviseert bij de ontwikkeling van diensten en producten en voorziet medewerkers desgevraagd van advies bij vraagstukken die aan het MVO beleid raken.

Iedere inbreuk op de gedragscode moet worden gerapporteerd volgens de procedures die namens de directie door de ethische commissie zijn vastgesteld. De directie verwacht van medewerkers dat zij iedere inbreuk, of een vermoeden daarvan, onder de aandacht van zowel de directie als de ethische commissie brengen, tenzij deze (vermoedelijke) inbreuk op één van beiden betrekking heeft. Er zijn maatregelen genomen om medewerkers in staat te stellen vertrouwelijk te rapporteren en geen enkele medewerker zal van het doen van een dergelijke melding nadeel ondervinden.

3. Privacy en misbruik van technologie

De producten en diensten die Fox-IT biedt zijn erop gericht om de samenleving veiliger te maken. Fox-IT levert dan ook geen producten en diensten ten behoeve van het onderdrukken of ontnemen van mensenrechten. Wanneer er een risico bestaat dat producten of diensten die door Fox-IT ontwikkeld worden misbruikt kunnen worden, treft Fox-IT alle redelijke maatregelen om dat te voorkomen.. De ethische commissie zal daarbij in een zo vroeg mogelijk stadium worden betrokken om advies uit te kunnen brengen.. Wij bouwen waar mogelijk privacybeschermende middelen in conform principes zoals *privacy by design*, bijvoorbeeld om communicatie met geheimhouders uit te zonderen.[4] Ook zorgen wij er zoveel mogelijk voor dat geleverde producten niet door derden misbruikt kunnen worden. Om inzichtelijk te maken hoe Fox-IT zijn maatschappelijk verantwoordelijkheid neemt, wordt hierna verdere uitleg gegeven over onze werkwijze op de maatschappelijk meest relevante punten.

Digitaal binnendringen

Fox-IT voert regelmatig penetratietesten uit bij opdrachtgevers. Een "pentest" is een geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken, om inzicht

[4] Een geheimhouder is iemand die in zijn dagelijkse beroep verplicht is tot geheimhouding. Burgers moeten erop kunnen vertrouwen dat gesprekken die zij voeren met artsen, advocaten, notarissen of geestelijk raadslieden geheim blijven.

te krijgen in de mate van kwetsbaarheid van dat systeem en om verbeterpunten te definiëren. Wanneer klanten ons vragen om hun beveiliging te testen door middel van een pentest, maken wij op verzoek van de klant binnen het kader van de opdracht soms gebruik van middelen met een heimelijke werking (social engineering). Wij verkopen echter geen Trojaanse paarden en brengen ook geen *back doors* aan in onze eigen producten.

Door de technologische vooruitgang en de digitalisering van de maatschappij hebben opsporende instanties andere bevoegdheden nodig. Overheden zouden cybercriminaliteit kunnen beperken door binnen te dringen in systemen die verantwoordelijk zijn voor het uitvoeren van een aanval. Onder huidig recht is "terughacken" meestal geen gelegitimeerde opsporingsmethode. Bovendien kan het binnendringen in een systeem worden gezien als een inmenging op het privacyrecht.[5] Het is daarom van belang dat een eventuele uitbreiding van bevoegdheden gepaard gaat met de juiste waarborgen. Fox-IT wil bij de technische invulling van deze bevoegdheden en waarborgen een evenwichtige rol spelen.

Het gericht inzetten van technische middelen tegen (de systemen van) verdachten van bepaalde ernstige strafbare feiten verdient wat Fox-IT betreft de voorkeur boven het ongericht inzetten van technische middelen. Eventuele nieuwe bevoegdheden moeten met voldoende waarborgen worden omkleed, om ervoor te zorgen dat de inbreuk op de persoonlijke levenssfeer zo veel mogelijk wordt beperkt. Daarnaast dienen de ingezette middelen proportioneel te zijn. Als de inzet van terughacken wettelijk wordt vastgelegd en Fox-IT in een specifiek geval om medewerking wordt gevraagd, dan zal Fox-IT een eigen afweging maken over het inzetten van onze middelen. Eventuele individuele afwegingen van medewerkers om daaraan geen medewerking te verlenen zullen worden gerespecteerd. Wij zullen klanten altijd wijzen op methodes die zo weinig mogelijk inbreuk maken op privacy.

Beveiligingsonderzoek en zero days

Medewerkers van Fox-IT voeren regelmatig beveiligingsonderzoek uit. Als wij hierbij nog niet publiek bekende kwetsbaarheden ontdekken (*zero days*[6]), informeren wij onze klanten en zo mogelijk de betrokken producent daarover. Wij zorgen ervoor dat de kwetsbaarheden volgens ons *responsible disclosure* beleid worden opgelost, tenzij dit tijdelijk of blijvend onmogelijk is door strijdigheid met het legitieme belang van onze klanten.[7] Fox-IT verkoopt geen exploits voor kwetsbaarheden.

---

[5] M.E. Koning, *Terug-hacken als opsporingsmethode: Een juridische analyse van de terughack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling*, (Amsterdam: Universiteit van Amsterdam, 2011).

[6] Een *zero day* is een kwetsbaarheid in software die ontdekt wordt door derden, buiten de maker van de software om, waarvoor nog geen patch voorhanden is. Hackers kunnen door middel van een *exploit* voor een dergelijke kwetsbaarheid de vertrouwelijkheid, integriteit of beschikbaarheid van systemen en/of gegevens negatief beïnvloeden, zonder dat de maatschappij zich daar afdoende tegen kan beschermen.

[7] *Responsible disclosure* is het op een verantwoorde wijze en zo mogelijk in gezamenlijkheid tussen melder en producent openbaar maken van ICT-kwetsbaarheden op basis van een daarvoor vastgesteld beleid.

Interceptie van dataverkeer

Fox-IT levert diensten en producten voor het bewerken van data die gericht en rechtmatig is verkregen. Deze bewerkingen hebben tot doel om de verkregen data inzichtelijk te maken, waarbij gebruik kan worden gemaakt van *deep packet inspection*.[8] Met onze diensten staat Fox-IT partijen bij die kwaadaardige activiteiten in hun eigen infrastructuur willen opsporen.[9] Wij voldoen aan alle wettelijke eisen op dit gebied en verwachten van onze klanten dat zij gebruikers op hun netwerk goed informeren over de toepasselijke beveiligingsmaatregelen. Fox-IT levert geen producten of diensten die bijdragen aan de massasurveillance van burgers door overheden.

Dual use

Zogenaamde dual-use beveiligingstechnologieën kunnen op verschillende manieren gebruikt worden. De handel in dual-use beveiligingstechnologieën wordt onder andere gereguleerd door het Wassenaar Arrangement, de Europese dual-use verordening en regels van de Nederlandse Rijksoverheid inzake dual-use goederen.[10] Fox-IT houdt zich aan deze regels en wil dat er verdere multilaterale afspraken gemaakt worden om misbruik van dual-use technologieën tegen te gaan.

4. Klanten

Fox-IT streeft naar een veiligere (inter)nationale samenleving, waarin het respecteren van mensenrechten centraal staat. Fox-IT beschermt zijn klanten tegen allerlei vormen van cybercrime. De producten en diensten van Fox-IT beschermen bijvoorbeeld bankgegevens van consumenten, voorkomen bedrijfsspionage, verdedigen vitale infrastructuur en stellen (staats)geheimen veilig. Fox-IT beperkt technisch misbruik van haar producten door waar mogelijk privacybeschermende middelen in te bouwen, door open te zijn over technologie en door producten steeds te verbeteren.

Fox-IT werkt voor de private en de publieke sector. De dienstverlening van Fox-IT is onder meer gericht op het beveiligen van vitale infrastructuur, zoals de energie, financiële - en telecommunicatiesector.[11] De Nederlandse overheid is één van de klanten van Fox-IT. Fox-

---

[8] Bij *deep packet inspection* wordt elektronisch dataverkeer tussen zender en ontvanger inhoudelijk geanalyseerd.

[9] In deze categorie levert Fox-IT de diensten ProtACT en DetACT. Deze diensten hebben als doel om respectievelijk kwaadaardige netwerkactiviteit en financiële fraude te detecteren.

[10] Raad van de Europese Unie, *Verordening (EG) Nr. 428/2009 van de Raad tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeërlei gebruik* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2009R0428:20120615:NL:PDF>.
Rijksoverheid, *Regels voor export en doorvoer van dual-use goederen* <http://www.rijksoverheid.nl/onderwerpen/exportcontrole-strategische-goederen/dual-use-goederen >.

[11] Vitale infrastructuren zijn ketens van vergelijkbare partijen waarvan het vanuit maatschappelijk oogpunt cruciaal is dat zij blijven functioneren.

IT werkt ook voor overheden in andere landen. Vertrouwelijkheid is één van Fox-IT's belangrijkste waarden. Fox-IT zal daarom niet de identiteit van specifieke klanten prijsgeven zonder uitdrukkelijke toestemming, tenzij dit bijvoorbeeld noodzakelijk is om te voldoen aan de wet. Wij kunnen wel inzicht geven hoe Fox-IT toetst of projecten op een verantwoorde manier geleverd kunnen worden aan klanten. De ethische commissie kan daarbij gevraagd of ongevraagd advies geven, waarbij een risicoanalyse plaats vindt ten aanzien van het specifieke geval. De directie zal het advies van de ethische commissie steeds bij haar besluitvorming betrekken. De directie is eindverantwoordelijk voor het gevoerde beleid en de keuzes die in specifieke gevallen worden gemaakt.

Fox-IT maakt gebruik van het navolgende toetsingskader, waarin een onderscheid wordt gemaakt tussen vier type actoren, namelijk inlichtingen- en veiligheidsdiensten, (de rest van) het veiligheidsapparaat, (de rest van) de overheid en de private sector. Het veiligheidsapparaat verwijst naar het deel van de overheid waarmee coërcieve macht uitgeoefend wordt en omvat tenminste de politie, openbaar aanklager en de krijgsmacht. Om te beoordelen in hoeverre overheden de politieke rechten en burgerlijke vrijheden van hun burgers respecteren sluit Fox-IT zich aan bij de *Freedom in the World* ranking van Freedom House (`http://freedomhouse.org/report-types/freedom-world/`), waarbij overheden worden aangemerkt als "*not free*", "*partly free*" of "*free*".

1. Fox-IT houdt zich aan de Nederlandse en Europese exportrestricties die van toepassing zijn op onze producten en/of diensten. Indien het gaat om een product dat voor meerdere doeleinden gebruikt kan worden, is Fox-IT bijvoorbeeld gebonden aan de regels voor export voor dual-use goederen (zie §3). De verplichting om deze en de navolgende restricties na te leven wordt ook opgenomen in de contracten met resellers en distributeurs.
2. Fox-IT levert producten en diensten alleen als redelijkerwijs verondersteld mag worden dat deze producten of diensten niet misbruikt zullen worden om mensenrechten te schenden. Bij de beoordeling of producten of diensten aan een klant geleverd kunnen worden spelen de aard van het product of dienst, de intenties van de klant en het in Fox-IT gestelde vertrouwen een belangrijke rol. Het toetsingskader geeft op de volgende wijze invulling aan dit principe:
    a. In landen die als "*not free*" worden aangemerkt worden geen producten en diensten geleverd aan inlichtingen- en veiligheidsdiensten of het veiligheidsapparaat. Voordat producten of diensten worden geleverd aan de rest van de overheid in deze landen zal de ethische commissie om advies worden gevraagd.
    b. In landen die als "*partly free*" worden aangemerkt worden producten en diensten aan inlichtingen- en veiligheidsdiensten of het veiligheidsapparaat alleen geleverd na een advies van de ethische commissie. Levering van producten en en diensten aan de rest van de overheid is in deze landen behoudens contra-indicaties zonder advies mogelijk.
    c. In landen die als "*free*" worden aangemerkt worden producten en diensten aan inlichtingen- en veiligheidsdiensten alleen geleverd na een advies van de

ethische commissie. Levering van producten en diensten aan het veiligheidsapparaat en de rest van de overheid is in deze landen behoudens contra-indicaties zonder advies mogelijk.

d. Levering van producten en diensten aan de private sector is in principe mogelijk ongeacht het land waarin ondernemingen gevestigd zijn. Als er echter redelijkerwijs vermoed wordt dat producten en diensten van Fox-IT door een actor misbruikt zouden worden, dan zal de ethische commissie voor levering om advies worden gevraagd. Als er onduidelijkheid bestaat over de feitelijke inzet van een product of dienst of een actor zich schuldig heeft gemaakt aan mensenrechtenschendingen, levert Fox-IT dit product of deze dienst alleen als alle in redelijkheid te verwachten scenario's in overeenstemming zijn met de genoemde criteria.

3. Onze klanten stellen hun vertrouwen in Fox-IT en Fox-IT verbindt zich dit vertrouwen niet te beschamen. Fox-IT gaat al dan niet banden aan met (nieuwe) klanten op basis van een zorgvuldige afweging, zoals bedoeld in lid 2. Uitgangspunten en situaties kunnen snel wijzigen, of nieuwe informatie kan aan het licht komen, zodat eerder gemaakte afwegingen niet meer voldoen. In dergelijke gevallen zal de directie een nieuwe analyse en nieuwe afweging maken. De ethische commissie zal worden verzocht met dit doel een advies uit te brengen.
4. De directie zal in alle genoemde gevallen het advies van de ethische commissie in de besluitvorming betrekken en een weloverwogen afweging maken.
5. Jaarlijks wordt door middel van een transparantierapport geanonimiseerd inzicht gegeven in de wijze waarop en de mate waarin het toetsingskader wordt gehanteerd.

Herziening

Dit beleid wordt periodiek getoetst, herzien en aangepast, in overeenstemming met de nieuwste technologische ontwikkelingen en ons voortschrijdend inzicht. De laatste versie van ons MVO beleid is te vinden op: `https://fox-it.com/`

Datum: 2 maart 2015

Plaats: Delft

Ad Scheepbouwer Jurjen Harskamp Menno van der Marel Ronald Prins