Leidraad Uitwisseling van gevoelige informatie

Juni 2009

1. Doel van de Leidraad

Niet alle informatie is vrij toegankelijk voor een ieder; sommige informatie moet voor anderen onbekend blijven. Om te komen tot een veilige uitwisseling van gevoelige informatie is het essentieel een aantal gedragsregels of omgangsvormen met elkaar af te spreken. Deze Leidraad is een suggestie hoe gehandeld kan worden bij de vrijwillige uitwisseling van informatie. Partners kunnen gezamenlijk beslissen de gevoelige informatie uit te wisselen in overeenstemming met de voorgestelde afspraken in deze Leidraad. Met het aanvaarden van de voorgestelde afspraken uit deze Leidraad, verplichten de aan de uitwisseling van informatie deelnemende partijen zich dan wel naar de gestelde regels te handelen.

De keuze is vrijwillig, maar daarna is het naleven niet meer vrijblijvend.

De Leidraad heeft tot doel de uitwisseling van gevoelige informatie tussen bedrijven, instellingen en overheden op een veilige manier te laten verlopen. Op deze wijze wordt een bijdrage geleverd aan de beveiliging en de continuïteit van de deelnemende bedrijven, overheden en instellingen, waarbij misbruik van de informatie kan leiden tot onaanvaardbare schade.

De op een veilige manier gedeelde gevoelige informatie draagt bij aan kwalitatief betere discussies, oplossingen en uiteindelijk besluitvorming.

Het leidende principe is “do ut des” (ik geef opdat jij geeft).

2. Principes en intenties

2.1. Algemeen

1. De deelnemende partijen stellen zich ten doel hun eigen veiligheid op alle mogelijke manieren te versterken. In dit verband bestaat er een voortdurende behoefte aan uitwisseling van gevoelige informatie tussen de deelnemers.
2. De partijen zijn zich ervan bewust dat een dergelijke uitwisseling van gevoelige informatie passende beveiligingsmaatregelen vereist en zijn bereid daarvoor te investeren.
3. Informatie-uitwisseling in overeenstemming met deze Leidraad vindt uitsluitend plaats tussen bedrijven, instellingen en overheden die een door hun directie vastgesteld informatiebeveiligingsbeleid hanteren.
4. De directie van de deelnemende bedrijven, instellingen en overheden stellen procedures vast, die toegepast worden indien bewezen is of vermoed wordt dat het vertrouwelijke karakter van de in deze overeenkomst bedoelde gevoelige informatie is aangetast, inclusief de wijze waarop andere partijen van de omstandigheden en de getroffen maatregelen in kennis wordt gesteld.
5. Indien deelnemers aan de uitwisseling van gevoelige informatie zich niet houden aan de gemaakte afspraken kunnen op hen (en hun bedrijf) de genoemde sancties van toepassing zijn, waaronder royering uit het overleg.
6. Met het werken in overeenstemming met deze Leidraad verplichten de deelnemende partijen zich (moreel) naar de gestelde regels te handelen. De verstrekker geeft informatie op vrijwillige basis, maar de ontvanger kan daar niet vrijblijvend mee om gaan. De informatie-uitwisseling is wederzijds op basis van gedeelde intenties.
7. Deelnemers staan andere deelnemers toe - onder condities - kennis te nemen van het informatiebeveiligingsbeleid van hun bedrijf, instelling of overheid.

2.2. De verstrekker

8. De verstrekker beslist binnen de kaders van het informatiebeveiligingsbeleid van zijn bedrijf, instelling of overheid, welke gevoelige informatie gedeeld mag / kan worden met andere deelnemers. Daarbij wordt onder meer een afweging gemaakt van de concurrentieaspecten in relatie tot de vitale belangen van het geheel.

9. De verstrekker geeft aan welke gevoeligheidswaardering zijn informatie heeft en welke (extra) voorwaarden hij aan de behandeling van die informatie stelt.
10. De leverende partij is zich ervan bewust dat, indien de ontvangende partij een bestuursorgaan betreft, de verstrekte informatie opgevraagd kan worden met een beroep op de Wet openbaarheid van bestuur. Partijen dienen vooraf duidelijk en gemotiveerd de gevoelige delen van de informatie te benoemen, zodat een beroep op de uitsluitinggronden kan worden gedaan bij verzoek tot openbaarmaking.

2.3. De ontvanger

11. De ontvanger beoordeelt vooraf of hij de aangeboden informatie wil en kan ontvangen en of hij daar op de vereiste wijze mee om kan gaan.
12. De ontvanger behandelt de informatie in overeenstemming met de door de verstrekker aangegeven gevoeligheid. De verstrekte informatie krijgt van de ontvanger een rubricering die minimaal gelijkwaardig is met de rubricering die de verstrekker er aan gegeven heeft.
13. Voor het vrijgeven of bekendmaken van de gerubriceerde informatie aan anderen dan de deelnemers aan een uitwisseling, is toestemming vereist van de leverende partij (zogenoemde derdepartijenregel).
14. De ontvanger gebruikt de in deze overeenkomst bedoelde gerubriceerde informatie niet voor andere doeleinden dan die welke zijn vastgesteld door de leverende partij.
15. Wanneer de ontvanger ontdekt (of concludeert) dat de ontvangen informatie niet op de door de verstrekker vereiste wijze is behandeld, meldt hij dit onverwijld aan de verstrekker.

3. Het referentiekader

3.1. Begrippen: gevoelig en gerubriceerd

Er bestaan verschillende termen voor hetzelfde begrip, maar ook eenzelfde term is voor meerdere uitleg vatbaar. Dat leidt tot onduidelijkheid en verwarring. Daarom is het belangrijk om een unité de doctrine te hanteren. Deze Leidraad sluit aan bij de termen die in Europees verband in de EPCIP[1] - richtlijn[2] worden gebruikt. Daarin wordt gesproken over gevoelige informatie; in het Engels: sensitive information. Er zijn gradaties aan te brengen in de mate van gevoeligheid. In deze Leidraad wordt daar het begrip "gerubriceerd" voor gebruikt; in het Engels: classified. Gerubriceerde informatie is daarmee per definitie gevoelige informatie.

3.2. Kleurencodering

Door bedrijven, instellingen en overheden worden verschillende termen gebruikt, waarbij de termen onderling niet altijd van gelijke gevoeligheidswaarde zijn en/of de maatregelen niet gelijkwaardig zijn. Om het mogelijk te maken een gezamenlijke "taal" te hanteren, is in deze Leidraad een generiek te gebruiken referentiekader opgesteld. Bedrijven, instellingen en overheden kunnen hun eigen rubricering afzetten tegen dit referentiekader en zo een evenwichtige vergelijking maken.

In deze Leidraad wordt voor een eenduidige aanduiding gebruik gemaakt van een kleurencodering, zoals ook enkele andere organisaties die gebruiken. De te gebruiken kleuren (wit, groen, geel en rood) hebben een associatie van veilig tot onveilig. Deze kleuren geven direct een beeld van de gevoeligheidswaarde van de informatie. Bij de kleuren wordt ter versterking tussen haken nog een tekst toegevoegd.

3.3. Overige gevoelige informatie

Aangenomen wordt dat in besprekingen die gehouden worden onder deze Leidraad, geen informatie met een hogere gevoeligheid dan de rubricering 'rood' wordt uitgewisseld.

---

1 European Programme for Critical Infrastructure Protection

2 EPCIP richtlijn 2008/114/EG van de raad, 8 december 2008 artikel 2, lid d

GEEL > VERTROUWELIJK

Uitwisseling

De informatie is alleen toegankelijk voor een selecte groep van direct betrokken personen, bijvoorbeeld voor deelnemers aan de specifieke besprekingen. Zij mogen de informatie ook delen met mensen binnen hun organisatie die deze informatie nodig hebben, hetzij om maatregelen te treffen of om een bijdrage te kunnen leveren aan de discussie en meningsvorming van de deelnemer.

Indicatie

Informatie waarvan kennisneming door niet gerechtigden:

- *schade toebrengt of zou kunnen toebrengen aan het bedrijf, de overheid of de instelling (imagoschade, financiële schade met consequenties voor liquiditeit, klachten en schadeclaims of wordt betrokken bij rechtsvervolging) of*
- *de relatie met andere bedrijven, instellingen en overheden of partners beschadigt of kan beschadigen.*

ROOD > GEHEIM

Uitwisseling

De informatie is uitsluitend toegankelijk voor geselecteerde personen die zijn aangewezen door, of bekend zijn bij, de informatie-eigenaar. De informatie wordt in principe mondeling gedeeld. Indien de informatie uitwisseling schriftelijk of elektronisch plaatsvindt, worden expliciet afspraken gemaakt over de beveiliging van de informatie, onderdeel daarvan is borging dat de geadresseerde ook de juiste en enige ontvanger is.

Indicatie

Informatie waarvan kennisneming door niet gerechtigden:

- *ernstige schade toebrengt of zou kunnen toebrengen aan het bedrijf, de instelling of de overheid (leidt een substantieel verlies, komt internationaal onder druk te staan en / of het voortbestaan is in geding) of*
- *de relatie met andere bedrijven, organisaties of partners ernstig beschadigt of ernstig kan beschadigen.*

WIT > OPENBAAR

Uitwisseling

De informatie is specifiek gemaakt om openbaar te maken. Informatie is (op aanvraag) vrij toegankelijk of is vrijgegeven voor publicatie via openbare bronnen zoals internet en de pers. De eventuele auteursrechtelijke bepalingen blijven van kracht.

GROEN > BESLOTEN

Uitwisseling

De informatie is alleen toegankelijk voor een bepaalde groep van personen. De informatie mag worden gedeeld met andere organisaties, informatiefora of personen die werkzaam zijn in beveiligingsfuncties. De informatie mag niet openbaar gemaakt worden door publicatie of plaatsing op openbare websites.

Indicatie

Informatie waarvan kennisneming door niet gerechtigden:

- *leidt of kan leiden tot nadeel voor het bedrijf, de overheid of de instelling (dragelijk financieel verlies, irritatie bij partners, producten en diensten kunnen alleen met extra inspanning worden geleverd) of*
- *de relatie met andere bedrijven, instellingen en overheden of partners benadeelt of zou kunnen benadelen, of*
- *leidt tot of kan leiden tot (ongewenste) openbaarmaking van gegevens of vermelding in pers.*

Daarom is er in deze Leidraad geen aanduiding voor informatie met een hogere gevoeligheid dan 'rood' (geheim).
Indien deelnemers van mening zijn dat informatie met een hogere gevoeligheid dan de kwalificatie met 'rood' gedeeld kan en moet worden, worden specifieke afspraken gemaakt voor de uitwisseling van informatie. De verstrekker bepaalt daarbij de te volgen gedragregels.

3.4. Vaststellen van standaard waardering

De mate van gevoeligheid en daarmee het van toepassing zijnde gevoeligheidsniveau, wordt door de opstellende organisatie vastgesteld in overeenstemming met de regels uit het eigen informatiebeveiligingsbeleid. Aanbevolen wordt om als standaard voor alle gevoelige informatie het niveau 'Geel (Vertrouwelijk)' te hanteren tenzij anders gespecificeerd. Daarmee is dan geborgd dat er zonder een andere beslissing een gedegen niveau staat.

3.5. Hogere waardering dan origineel

De verstrekker bepaalt het kleurniveau op basis van zijn beoordeling over de gevoeligheid van de verstrekking van de informatie. De ontvanger behandelt de ontvangen informatie naar de waarde van de kleur die het meegekregen heeft. Het kan zijn dat een verstrekker informatie die binnen zijn bedrijf de eigen rubricering op het equivalent 'Groen (besloten)' heeft, die ter beschikking wil stellen aan een specifiek persoon buiten zijn organisatie. De informatie heeft daarmee dan de rubricering 'Rood (geheim)'; het is immers voor uitsluitend die persoon bestemd.

3.6. Derubricering: lager waarderen

Een document waarvan een rubricering te hoog is om te (mogen) uitwisselen, kan lager ingedeeld worden als de informatie die de hoogste indeling bepaalt uit het document wordt gehaald. Dan is er sprake van derubricering. Ook kan door de loop van de tijd de gevoelige informatie aan waarde afnemen en leiden tot derubricering. Het is de eigenaar van de informatie die een lagere indeling in een rubriceringniveau aangeeft.

3.7. Cumulatie van gevoelige informatie

Door het samenvoegen van gevoelige informatie, kan de rubricering van deze bundeling hoger worden dan de hoogste rubricering van de afzonderlijke informatie-componenten. Wat eerst wit of groen was, kan door cumulatie mogelijk zelfs rood worden. De som is dan meer dan de losse delen.

De opsteller van het nieuwe document bepaalt, in samenspraak met de opdrachtgever, de nieuwe rubricering van het document. Het kan tot gevolg hebben dat door die toegenomen waarde van de verzameling en bewerking van de ontvangen informatie, het nieuwe document niet zonder meer met de oorspronkelijke verstrekkers gedeeld kan worden. De verstrekkers worden hier gemotiveerd over geïnformeerd.

4. Regels voor besprekingen en bijeenkomsten

Deze Leidraad is ook van toepassing op niet-schriftelijke informatie die uitgewisseld wordt tijdens besprekingen waarin gevoelige onderwerpen besproken worden. Bij het houden van besprekingen of bijeenkomsten moet rekening gehouden worden met de aard van de deelname (zie 4.1) en de wijze van informatie-uitwisseling. Expliciet wordt bij de uitwisseling van informatie tijdens besprekingen, bijeenkomsten of persoonlijke gesprekken aangegeven of conform deze Leidraad wordt gehandeld en zo ja, welke informatie onder welke rubricering valt.

Op verslagen, rapporten of andere vormen van schriftelijke weergave van de bespreking wordt vermeld of deze Leidraad van toepassing is en zo ja, welke informatie onder welke rubricering valt. Het document zelf heeft de rubricering van de zwaarst gerubriceerde gevoelige informatie uit het document.

4.1. Open of geselecteerde deelname

Wanneer er bijeenkomsten worden gehouden, zijn er ruwweg drie vormen van deelname:

1. Vrije inschrijving of verschijnen;
2. Deelname op uitnodiging zonder geheimhouding en zonder specifieke afscherming / beveiliging (vervanging is beperkt mogelijk);
3. Deelname op uitnodiging met geheimhouding, met specifieke afscherming / beveiliging en zonder vervangers.

Bij punt 1. vindt er geen feitelijke selectie plaats op de deelnemers. Dit betreft vaak congressen en seminars. Ook onder andere pers, studenten en consultants kunnen deelnemen. Beoogde deelnemers kunnen zich ook laten vervangen door iemand anders. Bij dit soort bijeenkomsten kan in feite alleen informatie met de rubricering 'wit' (open) worden uitgewisseld.

Bij punt 2. vindt er een selectie plaatst naar een specifieke doelgroep. Deze deelnemers worden op naam uitgenodigd en zij kunnen zich ook niet - zonder vooroverleg - laten vervangen door iemand anders. Bij binnenkomst wordt aan de hand van een uitnodigingslijst gecontroleerd of de naam van de aanmelder op de lijst voorkomt. Niet van te voren aangemelde (en geaccepteerde) vervangers worden in principe niet toegelaten. Bij dit soort bijeenkomsten kan ook informatie met de rubricering 'groen' (besloten) worden uitgewisseld.

Punt 3. Is een restrictiever vorm met uitnodiging op persoon. De deelnemende personen zijn bij naam en toenaam bekend of legitimeren zich bij binnenkomst. Er zijn voorzieningen getroffen voor de afscherming en beveiliging onder meer ten aanzien van de catering, technische ondersteuning en vernietiging van aantekeningen. Deze bijeenkomsten zijn bedoeld om de mogelijkheid te hebben om informatie met de rubricering 'geel' (vertrouwelijk) en in bijzondere situaties 'rood' (geheim) uit te wisselen.

4.2. Open bespreking

Alle gedeelde informatie is vrij te gebruiken, onder de gebruikelijke regels van bronvermelding.

4.3. Bespreking onder Chatham house rule

Wanneer een bijeenkomst, of een deel ervan, wordt gehouden onder de Chatham House Rule[3] staat het deelnemers vrij de informatie uit de discussies te gebruiken, maar het is niet toegestaan die informatie te linken aan de identiteit van (een van) de deelnemers of de organisatie waaraan zij verbonden zijn.

Het stelt mensen in staat te spreken als individueel persoon, meningen kunnen worden gegeven die niet de mening van het eigen bedrijf hoeven te zijn. Het bevordert de vrije discussie. Het stelt de deelnemers ook in staat informatie en ervaringen te delen die op geen enkele wijze buiten de bijeenkomst herleidbaar mogen worden naar het eigen bedrijf.

3 http://www.chathamhouse.org.uk/about/chathamhouserule/

Mensen voelen zich doorgaans vrij en ontspannen als zij zich geen zorgen hoeven te maken over hun reputatie of de gevolgen van wanneer zij publiek geciteerd zouden worden. Op geen enkele wijze wordt tijdens een dergelijke bijeenkomst geluid- of beeld-opnamen gemaakt.

4.4. Restrictieve bespreking

Deelnemers mogen op geen enkele wijze ook maar iets openbaar maken van de informatie die gedeeld werd tijdens de bijeenkomst. Op geen enkele wijze wordt tijdens een dergelijke bijeenkomst geluid- of beeldopnamen gemaakt. De gemaakte aantekeningen worden vernietigd.

5. Sancties

De mogelijkheid van het treffen van sancties zet kracht bij de waarde van de gemaakte afspraken.

5.1. Royering van deelname

Indien deelnemers zich niet conformeren aan de gedragsregels uit deze Leidraad, worden zij niet meer toegelaten tot besprekingen en bijeenkomsten waar deze Leidraad op van toepassing is, of wordt verklaard.
De beslissing hiertoe wordt genomen door de deelnemers aan het overleg, veelal bij monde van de voorzitter. Het staat de voorzitter vrij om te beoordelen of de mate van schending van het gegeven vertrouwen zo is dat hij voorzitters van andere overeenkomstige overleggen informeert.
Bij overtreding van de gedragsregels uit deze Leidraad kan eveneens worden besloten tot het volledig stopzetten van de uitwisseling van (schriftelijke) informatie met de betreffende deelnemer en mogelijk ook zijn bedrijf, instelling of overheid.

5.2. Bedrijfsinterne of branchemaatregel

De schending van de geheimhouding c.q. overtreding van de afspraken en gedragsregels uit deze Leidraad, kan ter kennis worden gebracht van de directie van het bedrijf, de instelling of de overheid. Het is aan de directie om binnen hun kaders gepaste interne of externe maatregelen te treffen. Ook zou een beroeps-, brancheorganisatie of certificeringinstelling passende maatregelen kunnen treffen.

5.3. Wettelijke strafbaarstelling

Er bestaat veel uiteenlopende wet- en regelgeving over de geheimhoudingsplicht. De generieke bepalingen staan in het Wetboek van strafrecht. In het Wetboek van strafrecht zijn enkele strafbepalingen opgenomen die betrekking hebben op het onbevoegd openbaar maken van geheimen. Enerzijds hebben deze strafbepalingen betrekking op het schenden van de geheimhouding dat in het belang van de staat of van zijn bondgenoten is geboden (artikel 98 e.v. van het Wetboek van strafrecht). Een ander artikel heeft betrekking op de schending van de meer generieke

geheime informatie, namelijk het bekend maken van bijzonderheden waarvan de geheimhouding is opgelegd (art 272 e.v. van het Wetboek van strafrecht).

5.4. Aansprakelijkheid

Naast de strafrechtelijke mogelijkheden, bestaat er ook de mogelijkheid van aansprakelijkheidsstelling op basis van de bepalingen uit het Burgerlijk wetboek. De (aantoonbaar) geleden schade kan via de rechter mogelijk op de veroorzaker verhaald worden. In het Burgerlijk wetboek (BW) is in titel 3 boek 6 bepaald in welke gevallen een persoon een onrechtmatige daad pleegt en aansprakelijk is voor de door een ander geleden schade.