Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Wet gegevens-verwerking en meldplicht cybersecurity

De Wet gegevensverwerking en meldplicht cybersecurity (hierna: Wgmc) treedt 1 oktober 2017 voor een belangrijk deel in werking.

De Wgmc regelt het volgende:

- **Taken en gegevensverwerking NCSC** De Wgmc legt taken vast die het Nationaal Cyber Security Centrum (NCSC) namens de minister (en volgens de huidige portefeuille de Staatssecretaris) van Veiligheid en Justitie vervult. In samenhang hiermee verstevigt de Wgmc de grondslag om in het kader van de uitoefening van die taken persoonsgegevens en andere gegevens te verwerken.
- **Vertrouwelijkheid** De Wgmc regelt de voorwaarden waaronder vertrouwelijke informatie betreffende aanbieders (waarover het NCSC bijvoorbeeld vanwege een incidentmelding beschikt) met derden kan worden gedeeld.
- **Meldplicht** De Wgmc introduceert een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna: ICT-incident). Deze meldplicht geldt alleen voor vitale aanbieders die aangewezen zijn in het Besluit meldplicht cybersecurity. De meldplicht treedt nog niet op 1 oktober a.s. in werking, om vitale aanbieders een overgangsperiode te gunnen.

Taken NCSC en gegevensverwerking

Wat zijn de in de Wgmc vastgelegde taken van het NCSC?

Om uitval van de beschikbaarheid of verlies van de integriteit van informatiesystemen van de doelgroep van het NCSC (rijksoverheid en bedrijven die deel uitmaken van de vitale infrastructuur) te voorkomen of beperken, en om de digitale weerbaarheid van de Nederlandse samenleving te versterken, heeft het NCSC de volgende taken:

- Bijstand verlenen aan de doelgroep bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van hun diensten te waarborgen of herstellen.
- Informeren en adviseren van de doelgroep en anderen (in en buiten Nederland) over dreigingen en incidenten met betrekking tot informatiesystemen van de doelgroep.
- Verrichten van analyses en technisch onderzoek ten behoeve van de hiervoor genoemde taken, naar aanleiding van bovengenoemde dreigingen en incidenten of aanwijzingen daarvoor (maar niet onderzoek naar de daarvoor verantwoordelijke personen of organisaties).

Daarnaast heeft het NCSC tot taak gegevens over dreigingen en incidenten betreffende andere systemen dan die van de doelgroep ('bijvangst') met bepaalde organisaties te delen. Dit wordt verder besproken onder "Wat regelt de Wgmc over 'bijvangst'?".

Wat regelt de Wgmc over de taken en gegevensverwerking door het NCSC?

Om de hierboven genoemde taken goed uit te kunnen oefenen verwerkt het NCSC veel gegevens. In de Wgmc is een steviger wettelijke grondslag opgenomen voor gegevensverwerking, gelet op het groeiend belang en de ontwikkeling van het NCSC, en de bevoegdheid om informatie bij andere organisaties op te vragen. Meer in het bijzonder geldt het volgende:

- De Wgmc legt vast (i) wat de taken van het NCSC zijn in het kader waarvan in elk geval ook persoonsgegevens worden verwerkt, en (ii) dat ten behoeve van die taken (persoons)gegevens kunnen worden verwerkt. Bij het verwerken van persoonsgegevens gaat het in beginsel alleen om die gegevens die noodzakelijk zijn voor het uitoefenen van deze taken. Denk hierbij aan bij dreigingen en incidenten betrokken IP-adressen, e mailadressen en domeinnamen, en contactgegevens van personen van organisaties die tot de doelgroep van het NCSC behoren.
- De Wgmc bepaalt dat het NCSC bij andere organisaties gegevens kan opvragen, als die noodzakelijk zijn voor het vervullen van de taken van het NCSC. Daarbij hebben die organisaties de mogelijkheid om in reactie op zo'n verzoek zo nodig ook persoonsgegevens te verstrekken.

Met het bovenstaande wordt ook duidelijker geregeld dat en wanneer het NCSC (persoons)gegevens met andere partijen kan delen en dus ook in dat opzicht invulling kan geven aan publiek-private samenwerking. Zie in dit verband ook hieronder "Vertrouwelijkheid van informatie".

Mag het NCSC ook onderzoek doen naar daders achter de ICT-incidenten?

Het NCSC mag geen onderzoek doen naar personen of organisaties die verantwoordelijk zijn voor dreigingen en incidenten of daar anderszins aan bijdragen of hebben bijgedragen. Het NCSC heeft nadrukkelijk niet tot taak om bijvoorbeeld de identiteit te achterhalen van diegenen die een dreiging of incident veroorzaken of veroorzaakt hebben. Dadergericht onderzoek is voorbehouden aan de inlichtingen- en veiligheidsdiensten, de politie en het OM.

Wel kan het NCSC bijvoorbeeld nagaan of een bij een incident betrokken IP-adres toebehoort aan een vitale aanbieder of aan een andere aanbieder die onderdeel is van de rijksoverheid (op basis van reeds bij het NCSC bekende IP-adressen van die aanbieders), zodat het die aanbieder kan waarschuwen.

Wat regelt de Wgmc over 'bijvangst'?

Bij de analyses en het technisch onderzoek naar aanleiding van dreigingen en incidenten betreffende de systemen van organisaties, die behoren tot de doelgroep van het NCSC, kunnen ook gegevens worden verkregen over dreigingen of incidenten met betrekking tot andere systemen dan doelgroeporganisaties ('bijvangst'). Daarbij kan het bijvoorbeeld gaan om e-mailadressen die door een ICT-incident kwetsbaar zijn geworden, die deel uitmaken van een dataset die het NCSC onderzoekt met het oog op de uitoefening van de reguliere taken. De Wgmc geeft het NCSC de bevoegdheid om, ter voorkoming van nadelige maatschappelijke gevolgen, dergelijke 'bijvangst' te delen met de volgende kring van ontvangers:

- Organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek over die (andere) dreigingen of incidenten te informeren.
- Bij ministeriële regeling aangewezen computercrisisteams.
- Aanbieders van internettoegangs- of internetcommunicatiediensten, ten behoeve van het informeren van gebruikers van die diensten.

Uit de privacywetgeving volgt bovendien dat persoonsgegevens alleen worden verstrekt, als dat noodzakelijk is gezien de aard en omvang van de gegevens en de mogelijke maatschappelijke gevolgen.

Vertrouwelijkheid van informatie

Het NCSC kan de beschikking krijgen over vertrouwelijke gegevens betreffende aanbieders. De Wgmc bevat een strikte regeling met betrekking tot het verstrekken van die vertrouwelijke gegevens aan derden. Het is om een aantal redenen van belang dat de vertrouwelijkheid van deze gegevens hierdoor zo veel mogelijk wordt gewaarborgd. Ten eerste garandeert de vertrouwelijkheid dat het NCSC deze gegevens kan gebruiken bij het uitvoeren van de wettelijke taken, zonder daarbij gehinderd te worden door vroegtijdig openbaar worden van deze gegevens. Daarnaast is het van belang om schade bij betrokken aanbieders, zoals reputatieschade of toegenomen kwetsbaarheid voor gerichte aanvallen, zo veel mogelijk te voorkomen. Deze regeling beoogt ook te voorkomen dat aanbieders terughoudend worden met het delen van vertrouwelijke informatie, omdat het NCSC bij terughoudendheid in ernstige mate zou worden benadeeld in het uitvoeren van zijn wettelijke taken.

Wat houden de regels met betrekking tot vertrouwelijkheid in?

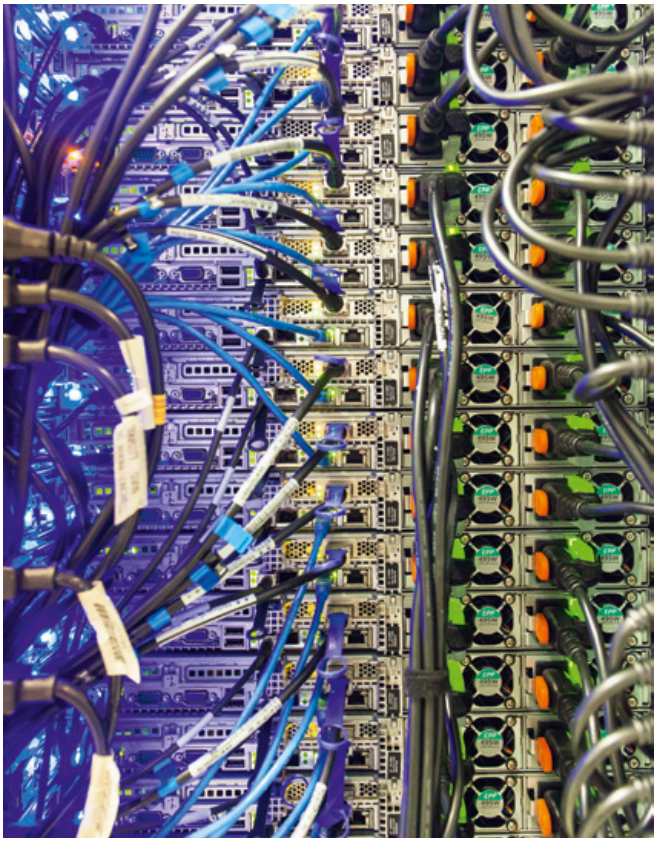
Vertrouwelijke gegevens betreffende een aanbieder worden slechts zonder toestemming van de aanbieder aan derden verstrekt, als de geheimhouding daarvan voldoende is gewaarborgd en bovendien gewaarborgd is dat de gegevens alleen worden gebruikt voor het doel waarvoor zij verstrekt worden.

Voor vertrouwelijke gegevens die bovendien herleid kunnen worden tot die aanbieder (bijvoorbeeld de naam van de aanbieder), geldt een nog striktere regeling. Deze gegevens kunnen zonder toestemming van de betrokken aanbieder slechts in een beperkte kring en in uitzonderlijke gevallen worden gedeeld.

Wanneer kan het NCSC wel vertrouwelijke herleidbare gegevens verstrekken?

Het NCSC heeft in de volgende situaties geen instemming van de aanbieder nodig om vertrouwelijke herleidbare gegevens betreffende die aanbieder aan derden te verstrekken:

- *Aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en aan daartoe bij ministeriële regeling aangewezen computercrisisteams:* voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer.
- *Aan de betrokken vakminister:* als een aanbieder adviezen van het NCSC niet opvolgt en daardoor het risico op maatschappelijke ontwrichting aanwezig blijft, of als dit noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken.
- *Aan andere organisaties of aan het publiek:* wanneer het noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken. In veel gevallen zal het publiek ook kunnen worden gewaarschuwd met een niet tot de aanbieder herleidbare mededeling, maar soms zal voorlichting alleen effectief kunnen zijn door de betrokken aanbieder wel te noemen, bijvoorbeeld als het nodig is te waarschuwen dat er grote risico's verbonden zijn aan het gebruik van een bepaald product of een bepaalde dienst. Het NCSC zal in deze gevallen de betrokken aanbieder vooraf raadplegen.



Kunnen vertrouwelijke gegevens opgevraagd worden door middel van een verzoek krachtens de Wet openbaarheid van bestuur (Wob)?

Voor vertrouwelijke herleidbare gegevens betreffende aanbieders regelt de Wgmc dat de Wob daarop niet van toepassing is. De Wob blijft wel van toepassing voor andere vertrouwelijke gegevens betreffende aanbieders.

Hoe verhouden de regels over vertrouwelijke gegevens in de Wgmc zich tot andere wetten?

De hierboven beschreven regeling in de Wgmc betreft alleen het (al dan niet) verstrekken van vertrouwelijke gegevens betreffende aanbieders, in het kader van de uitoefening van de taken door het NCSC. Het NCSC kan los daarvan verplicht zijn om deze gegevens te verstrekken uit hoofde van andere wetten, zoals artikel 8:28 Algemene wet bestuursrecht (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure) of artikel 126nc e.v. Wetboek van Strafvordering (vorderen van gegevens door officier van justitie).

Meldplicht

Wanneer geldt de meldplicht?

Als aan alle volgende voorwaarden is voldaan moet een melding van een incident worden gedaan bij het NCSC:

- Het gaat om een in het Besluit meldplicht cybersecurity aangewezen product of dienst van een in datzelfde besluit aangewezen vitale aanbieder.
- Er is of was een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem waarvan het product of de dienst afhankelijk is.
- Die inbreuk of dat verlies heeft geleid of kan leiden tot een onderbreking van de beschikbaarheid of de betrouwbaarheid van het product of de dienst.
- Die feitelijke of potentiële onderbreking moet belangrijk zijn, dus substantieel.

Meldingen dienen zo snel mogelijk te worden gedaan. De initiële melding kan beknopt zijn: liever een snelle melding die zo nodig later wordt aangevuld, dan een uitvoerige melding die op zich laat wachten.

Voor wie geldt de meldplicht?

Voor vitale aanbieders: overheidsorganisaties en privaatrechtelijke rechtspersonen die producten of diensten aanbieden waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving. De meldplicht geldt niet voor alle vitale aanbieders: het Besluit meldplicht cybersecurity zal de vitale aanbieders waarvoor de meldplicht gaat gelden aanwijzen, in relatie tot specifieke producten en diensten.

Waarom een meldplicht?

Een melding van een ICT-incident stelt het NCSC in staat om bijstand te verlenen aan de getroffen aanbieder. Verder kan het NCSC naar aanleiding van een melding van een incident andere aanbieders, die behoren tot de doelgroep van het NCSC, waarschuwen en adviseren. De melding stelt het NCSC in staat het risico van maatschappelijke ontwrichting in te schatten en door hulpverlening aan de doelgroep die ontwrichting te voorkomen of zo veel mogelijk te beperken.

Waar moet een melding worden gedaan en door wie wordt deze behandeld?

De melding van ICT-incidenten wordt formeel gedaan bij de Minister (volgens de huidige portefeuilleverdeling de Staatssecretaris) van Veiligheid en Justitie, en wordt in de praktijk ingediend bij en behandeld door het NCSC. Doe een melding altijd telefonisch via het bij u bekende alarmnummer van het NCSC. Stuur hierna direct een e-mail naar cert@ncsc.nl, onder vermelding van de meldplicht. De Wgmc verplicht een aanbieder die een melding heeft gedaan het NCSC desgevraagd nadere informatie te verschaffen, als die noodzakelijk is voor de hulpverlening of de inschatting van de risico's voor andere organisaties.

Wanneer wordt de meldplicht van kracht?

Het onderdeel in de Wgmc over de meldplicht treedt naar alle waarschijnlijkheid op 1 januari 2018 in werking. Het Besluit meldplicht cybersecurity treedt tegelijk in werking.

Wat als ik niet onder de meldplicht val, maar wel wil melden?

Organisaties die onder de doelgroep vallen kunnen ook incidenten die niet onder de meldplicht vallen vrijwillig melden bij het NCSC, als zij bijstand willen ontvangen van het NCSC. Het NCSC opereert 24/7 opereert als meldpunt voor cyberincidenten. Organisaties die niet tot de doelgroep van het NCSC behoren kunnen ook incidenten melden, maar ontvangen geen bijstand van het NCSC. Wel hebben zij toegang tot alle algemeen gepubliceerde beveiligingsadviezen en kennisproducten van het NCSC.

Verhouding tot EU-richtlijn netwerk- en informatiebeveiliging

Hoe verhoudt de Wgmc zich tot de EU-richtlijn voor Netwerk- en informatiebeveiliging?

Op dit moment wordt gewerkt aan de Cybersecuritywet,[1] ter uitvoering van de Europese richtlijn 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIB-richtlijn). De NIB-richtlijn regelt onder andere de plicht voor aanbieders van essentiële diensten (die vaak zullen overlappen met vitale aanbieders) om maatregelen te nemen om incidenten te voorkomen, een meldplicht in geval van ernstige incidenten bij zowel het NCSC als een toezichthouder, en toezicht op en handhaving van de naleving van deze plichten door de toezichthouder. De Wgmc zal zonder materiële wijzigingen in deze nieuwe Cybersecuritywet worden opgenomen.

Kijk voor informatie over de Wet gegevensverwerking en meldplicht cybersecurity op www.ncsc.nl/wgmc.

1 De consultatieversie is te vinden op www.internetconsultatie.nl/cybersecuritywet

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

september 2017