



**Consultation on draft bill regarding mandatory notification of ICT breaches in vital sectors / Consultatie wetsvoorstel inzake meldplicht ICT inbreuken vitale sectoren**

**5 August 2013**

*This newsletter is sent by NautaDutilh*

**Consultation on draft bill regarding mandatory notification of ICT breaches in vital sectors**

*A public consultation is currently ongoing on a draft bill for the introduction of mandatory notification of ICT breaches in vital sectors (name of proposed legislation in Dutch: Wet melding inbreuken elektronische informatiesystemen). The consultation opened on 22 July 2013 and will terminate on 17 September 2013. The draft bill does not provide for the imposition of sanctions.*

*The notification duty will only apply to providers of products or services whose availability or reliability are of vital importance for Dutch society (i.e. in sectors such as electricity, gas, water, telecommunications, finance, government and transport) and where the breach in question will or may have a significantly negative effect on the availability or reliability of the relevant product(s) or service(s). The duty will apply with respect to elements of vital infrastructure the breakdown of which would directly or indirectly lead to social disruption. The providers who will be subject to the duty will be designated by general administrative order (algemene maatregel van bestuur).*

*The relevant providers will include energy network managers, drinking-water companies, telecommunication companies, surface-water management bodies, banks, the operators of the port of Rotterdam (Havenbedrijf Rotterdam) and Schiphol airport (NV Luchthaven Schiphol), and the body responsible for air traffic control in the Netherlands (Luchtverkeersleiding Nederland). In the case of providers of certification services, a different system for the notification of ICT breaches will be put in place.*

Notifications must be made to the Minister of Security and Justice immediately, and will be handled by the National Cyber Security Centre (NCSC), which forms part of the ministry. The purpose of the notification duty is to enable the NCSC to assess the risks posed by a breach and to assist the provider affected by the breach, with the ultimate aim of preventing or limiting any social disruption. The information notified may also be used for advice and communications to other providers in vital sectors and the public at large. For example, a warning can be issued about the risks posed by a method of operation used by internet criminals, or recommending that a particular product or service not be used until further notice.

The notification shall in any event include:

- a. the nature and extent of the breach (of security) or the loss (of integrity of an information system) that will or may have a significantly negative effect on the availability or reliability of the relevant product(s) or service(s);
- b. the time of commencement of the breach or loss;
- c. the possible consequences of the breach or loss;
- d. a prognosis of the time it will take to remedy the breach or loss;
- e. if possible, the measures taken or to be taken by the provider in order to limit the consequences of, or prevent a repetition of, the breach or loss;
- f. the contact details of the officer based in the Netherlands who is responsible for giving the notification.

If so requested, a provider that has given a notification shall immediately provide the Minister with all other information that is necessary for the purpose of:

- a. assessing the risks to the availability or reliability of the product or service;
- b. assisting the provider with the taking of measures to secure or restore the availability and reliability of the product or service.

The NCSC will not be supervising compliance with the notification duty and will not have any powers of enforcement. Its primary role will be to offer assistance. The NCSC can, however, inform the authorities with competence in the relevant sector if it appears that there has been an intentional lack of compliance with the notification duty. Such authorities can then decide whether or not the non-compliance is reason for them to adopt a stricter supervision of that sector. If it turns out that there is insufficient compliance with the notification duty, it may be decided to arrange for a system of supervision and enforcement.

[Click here for \(in Dutch\):](#)

[Draft bill](#)

[Draft explanatory memorandum](#)

### **Consultatie wetsvoorstel inzake meldplicht ICT inbreuken vitale sectoren**

*Het wetsvoorstel (Wet melding inbreuken elektronische informatiesystemen) introduceert een meldplicht voor ICT inbreuken en is op 22 juli 2013 ter consultatie aangeboden. De einddatum van de consultatie is 17 september 2013. Het wetsvoorstel voorziet niet in de mogelijkheid van sanctionering.*

*De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, en alleen als de inbreuk tot gevolg heeft of kan hebben dat die beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. Deze aanbieders van vitale producten of diensten bevinden zich binnen de sectoren elektriciteit, gas, drinkwater, telecom, kerens en beheren oppervlaktewater, financiën, overheid en transport, zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterringen, banken, het Havenbedrijf Rotterdam, de NV Luchthaven Schiphol en luchtverkeersleiding Nederland. Het gaat om onderdelen van de vitale infrastructuur waarbij een ICT inbreuk direct of indirect tot maatschappelijke ontwrichting kan leiden. De aanbieders worden bij algemene maatregel van bestuur aangewezen. Voor certificaatsdienstverleners zal de melding van ICT inbreuken langs andere weg worden vorm gegeven.*

De melding moet (onverwijld) worden gedaan aan de Minister van Veiligheid en Justitie. De melding wordt behandeld door het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het ministerie. De meldplicht heeft primair tot doel om het NCSC in staat te stellen om de risico's van de ICT inbreuk te kunnen inschatten en de door de inbreuk getroffen aanbieder bij te staan met als uiteindelijk doel het voorkomen of beperken van maatschappelijke ontwrichting. De verstrekte gegevens mogen vervolgens ook worden gebruikt als basis voor advies en informatie aan andere vitale aanbieders en het publiek. Dit laatste kan bijvoorbeeld inhouden dat wordt gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze of dat wordt gewaarschuwd dat een bepaald product of een bepaalde dienst tot nader order beter niet kan worden gebruikt.

De melding die moet worden gedaan omvat in ieder geval:

- a. de aard en omvang van de inbreuk (op de veiligheid) of het verlies (van integriteit van een informatiesysteem) waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken;
- b. het tijdstip van de aanvang van de inbreuk of het verlies;
- c. de mogelijke gevolgen van de inbreuk of het verlies;
- d. een prognose van de hersteltijd;
- e. zo mogelijk de door de aanbieder genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;
- f. de contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.

Desgevraagd verstrekt de aanbieder die een melding heeft gedaan, de Minister onverwijld alle overige gegevens die nodig zijn om:

- a. de risico's voor de beschikbaarheid of betrouwbaarheid van het product of de dienst in te schatten;
- b. de aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het product of de dienst te waarborgen of te herstellen.

Het NCSC gaat geen toezicht houden op de naleving van de meldplicht en krijgt ook geen handhavingsbevoegdheden. Het NSCS is primair gericht op het bieden van hulp. Wel kan het NCSC de instanties die belast zijn met het toezicht op de naleving door de betrokken aanbieder van de op hem van toepassing zijnde wetgeving informeren als blijkt dat de meldplicht opzettelijk niet is nageleefd. Aan de hand daarvan kan de sectorale toezichthouder besluiten of niet naleving van de meldplicht voor hem aanleiding vormt om het sectorale toezicht aan te scherpen. Mocht blijken dat de meldplicht onvoldoende wordt nageleefd, dan kan alsnog worden besloten tot het inrichten van een stelsel van toezicht en handhaving.

Lees hier voor:

[Concept regeling wetsvoorstel](#)

[Ontwerp toelichting memorie van toelichting](#)

## Contact

---

For the Netherlands / voor Nederland:

Jacqueline van Essen

T: +31 20 7171 714

For Belgium / voor België:

Julien Hick

T: +32 2 566 8518

For Luxembourg / voor Luxemburg:

Vincent Wellens

T +35 2 261 22934

Amsterdam · Brussels · London · Luxembourg · New York · Rotterdam

## Privacy / General conditions / Disclaimer

This publication highlights certain issues and is not intended to be comprehensive or to provide legal advice. NautaDutilh N.V. is not liable for any damage resulting from the information provided. Dutch law is applicable and disputes shall be submitted exclusively to the Amsterdam or Rotterdam District Court, at the plaintiff's option. To unsubscribe, please use the [unsubscribe option](#) or send an e-mail to [unsubscribe@newsletter-nautadutilh.com](mailto:unsubscribe@newsletter-nautadutilh.com). For information concerning the processing of your personal data we refer to our privacy policy [www.nautadutilh.com/privacy](http://www.nautadutilh.com/privacy).