CLIFFORD
CHANCE

Client briefing August 2013

New ICT breach notification requirements proposed in the Netherlands

The Dutch Minister of Security and Justice has issued a draft Act introducing new notification requirements in the event of security breaches of electronic information systems used in critical market sectors. These sectors include financial services, telecoms, energy, transport and government institutions. The new notification requirements are another step to further enhance the level of awareness, transparency and preparedness in both public and private organisations in the face of ongoing ICT related security incidents.

Introducing new security breach notification requirements

The Electronic Information System Breach Notification Act (*Wet melding inbreuken elektronische informatiesystemen*), as the draft Act is called, introduces an obligation to notify the Dutch National Cyber Security Centre (NCSC) in the event of breaches of the security or integrity of electronic information systems that are used to provide products or services considered vital to Dutch society.

It is envisaged that providers of these vital products and services subject to the notification requirements will be designated in the following sectors: energy (electricity, gas), telecoms, water management, financial services, government and transport. The providers will include banks, telecom operators, electricity and gas (transmission system) suppliers, drinking water companies, water management companies (main barrages), the Port of Rotterdam, Schiphol Airport and air traffic management.

The draft Act provides for the obligation to notify an actual breach of the security or integrity of the information systems concerned. Disruptions that may (temporarily) affect the availability of a system without compromising the security or integrity of the system, as may for instance be the case in the event of DDOS attacks, are not considered to be such a breach, although such disruptions may nevertheless be notified to the NCSC voluntarily. Not all security breaches have to be notified; only those that cause or may cause a serious disruption of the availability or reliability of the designated products or services. Notably, the NCSC is not accorded any rights to enforce the notification requirements. In this respect, the new requirements are deemed part of a current practice of voluntary exchange of information between the public and private sectors on issues of cyber security.

Upon a security breach notification, the Minister of Security and Justice may inform other providers, national computer emergency response teams (in the Netherlands or abroad) and the public to avoid or limit the damages resulting from the breach. Unless required to safeguard societal interests, any information shared with the general public will not identify specific providers, products or services.

National and EU regulatory framework

The new notification requirements aim to complement other existing or proposed network or system security breach notification requirements that

might apply to the providers concerned, such as those already included in the Act on Financial Supervision, those recently introduced in the Dutch Telecommunications Act and those currently proposed to be introduced in the Dutch Data Protection Act.

The draft Act precedes the finalisation of the so-called Network and Information Security Directive, proposed by the European Commission in February 2013 (COM (2013) 48 of 7 Feb. 2013). Among other things, that Directive sets forth similar security breach notification requirements, albeit for a potentially wider scope of market operators, including providers of information society services which enable the provision of other information society services (such as providers of e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services and application stores). The draft Directive furthermore instructs Member States to ensure that relevant operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations, guaranteeing a level of security appropriate to the risk presented and ensuring the continuity of the services underpinned by those networks and information systems. The proposed Directive is currently under review by the European Parliament and Council, and is not expected to enter into force before 2015.

Conclusion

These new security breach notification requirements are another step in the current increased regulatory efforts at both a national and EU level to further enhance the level of awareness, transparency and preparedness in both public and private organisations in the face of ongoing ICT related security incidents. The draft Act is open for public consultation through the Internet, closing 17 September 2013.

At Clifford Chance we have a wealth of experience in advising market players globally and in all sectors on ensuring regulatory compliance of their business critical operations and systems, whether in the context of security and privacy impact analyses, incident management processes, systems development and integration, cloud services, outsourcing transactions or otherwise. Please contact us if you would like to know more about our services and the cyber security related legal requirements relevant to your organisation.

Contacts

Alvin Khodabaks
T +31 20 711 9374
alvin.khodabaks
@cliffordchance.com

Jaap Tempelman
T +31 20 711 9192
jaap.tempelman
@cliffordchance.com