CLIFFORD
CHANCE

Client briefing June 2012

The amended Dutch Telecommunications Act – new rules on cookies, net neutrality and security

On 5 June 2012, a long awaited amendment to the Dutch Telecommunications Act (the "DTA") entered into force (the "Amendment"). The Amendment introduces much debated issues such as requirements regarding the use of cookies and net neutrality. It also introduces less controversial (but no less important) provisions governing security breach notifications, the universal services definition and consumer protection. This briefing shortly discusses the most important changes.

The Amendment implements several European telecommunications Directives (Directives 2009/136/EC and 2009/140/EC), be it significantly later than the prescribed implementation date of 25 May 2011. Infringement proceedings by the European Commission against the Dutch Government had in fact commenced already and can now, at long last, be withdrawn. Most changes under the Amendment have become effective as of 5 June 2012; a few – notably relating to elements of both the cookie and net neutrality rules – will enter into force on 1 January 2013.

Cookie legislation

A controversial element of the Amendment, due to the potential burden it may impose upon businesses, is the so-called “cookie provision” (Article 11.7a DTA). This provision states that a party seeking to remotely access or place data – such as cookies – on a user's computer via electronic communication networks must first obtain the informed consent of that user to do so.

Cookies that are solely intended to enable communications over a public telecommunications network or that are strictly necessary to provide the (information society) service requested by the user are exempt from the requirement of a user's prior informed consent. The new requirements are, therefore, particularly relevant for the use of (third party) tracking cookies as a means to identify users and to register their internet surfing behaviour for advertising purposes.

The manner in which a user's consent is to be obtained still poses some practical problems. Discussions during the legislative process at the European and national level indicate that features in existing internet browsers are insufficient to allow users to express their informed and explicit consent on a case-by-case basis, which is in effect what the cookie provision requires. The European Commission is in discussions with the software industry to evaluate possibilities to implement adequate consent mechanisms. In the meantime, the requirements and desired approach may differ per jurisdiction.

Topics

- Cookie legislation
- Net neutrality
- Security and confidentiality requirements
- Universal services
- Consumer protection measures

The Dutch implementation of the cookie provision furthermore contains the legal presumption – effective from 1 January 2013 – that accessing or storing data on user devices for the purpose of collecting, combining or analysing information about the use of information society services for commercial, charity or idealistic purposes, qualifies as the processing of personal data and is governed by the Dutch Data Protection Act (DPA). Unless the party using cookies can prove it is not processing personal data, the use of tracking cookies will then, among other things, require the *unambiguous* prior and informed consent of users and the registration at the Data Protection Authority (*College Bescherming Persoonsgegevens)*. Other requirements applicable under the DPA, such as data subjects' rights (ie the right to check and correct data) also come into play.

Net neutrality

The Amendment furthermore introduces provisions on net neutrality (Article 7.4a DTA), which will enter into force on 1 January 2013. These aim primarily to safeguard the non-discriminatory treatment of access to internet services and applications. Internet access providers are prohibited from blocking or slowing down access to services and applications on the Internet except in a limited number of situations, such as when necessary to (non-discriminatorily) manage congestions or to ensure the safety and integrity of services, networks or end-user terminal equipment. Notably, the Amendment also expressly states that providers may not base their rates on the services or applications offered or used via the internet access services they provide. These restrictions may necessitate a thorough rethink of some operators' current business cases. It is, for instance, not uncommon for mobile network operators to limit access to applications such as Skype and WhatsApp, which undermine their call and SMS revenues. A point of discussion is to what extent the DTA would nevertheless allow such a restricted service offering at differentiated rates to end-users who explicitly accept those terms, in the event the provider concerned also offers a fully unrestricted service.

Security and confidentiality requirements

The DTA already obliged public communications network and service providers to protect the personal data and privacy of their subscribers and users and implement adequate security measures to this end. The Amendment adds a duty to protect the confidentiality of communications and related data, which will become effective as of 1 January 2013. Providers must refrain from tapping, intercepting or otherwise inspecting the contents of communications, subject to a limited number of exceptions (ie explicit consent, network integrity and security, functional necessity or a legal obligation). This for instance prevents the use of technologies such as "deep packet inspection" to enable certain business or pricing models. Additionally, the Amendment introduces the obligation to take adequate measures to manage security and integrity risks related to the use of public networks and services to ensure their continued availability. Furthermore providers of networks carrying public telephony services must implement measures to warrant the availability of services in the event of a technical failure or outage of the electricity network.

The Amendment complements the aforementioned obligations with breach notification requirements. Providers in scope of the applicable requirements must maintain an overview of all security breaches involving personal data and must notify the relevant authorities of any breaches that negatively affect the protection of personal data and of a breach of safety or loss of integrity that materially threatens the continued availability of networks and services. Data subjects must be notified where a breach is likely to negatively affect their private life, and the public may be informed in the event of continuity breaches.

Universal services

The universal service provisions of the DTA seek to ensure that certain basic services of a minimum quality are made available to all end-users at reasonable terms, where the market would not otherwise supply these. The Amendment expands the scope of the universal service definition to include facilities affording end-users with physical disabilities equal access to public fixed telephony services, telephone directories and subscriber information services. These facilities include a text relay and video relay service for the hearing impaired and directory services accessible to the visually impaired.

Consumer protection measures

The Amendment introduces a number of other changes aimed at enhancing consumer protection. It changes the scope of different obligations that providers have towards consumers

such as information requirements and service requirements. Most importantly, providers of public telephone services are required to offer contracts without call start rates, with a charging base per second and with rates otherwise comparable to other contracts offered. The Amendment furthermore introduces restrictions on the ability of internet access providers to terminate access under contracts with consumers to a limited number of predefined circumstances. Al these changes may require contracts and general terms and conditions to be updated.

Contacts

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

Joeri Toet
joeri.toet@cliffordchance.com
+31 20 711 9394

Clifford Chance, Droogbak 1A, 1013 GE Amsterdam, PO Box 251, 1000 AG Amsterdam

www.cliffordchance.com