



## TABS™ Update Technology And Brands

April/June 2010

“TABS” is a trade mark of Beauchamps Solicitors

### Data Security Breach Code of Practice launched

Companies or individuals who are data controllers (as defined under the Data Protection Acts 1988 and 2003) should note that the Irish Data Protection Commissioner has published a draft Data Security Breach Code of Practice for public consultation. The Code was published in response to a recommendation of the Data Protection Review Group (“the Group”).

The Group was established by the Minister for Justice, Equality and Law Reform in 2008 to consider, amongst others, how to ensure that the reporting applications of organisations in relation to data security breaches are sufficiently robust to protect the rights of data subjects. The Group recommended that *“the reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the (Data Protection Commissioner), should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the (Data Protection Commissioner)”*.

Under the draft Code, all incidents of the loss of personal data must be reported to the Data Protection Office by the data controller, within two working days of their becoming aware of the incident, except where (a) the personal data was inaccessible due to being stored on encrypted equipment secured to a high standard with a strong password and the password was not accessible to unauthorised individuals; (b) a password was stored on equipment with a strong password and a remote memory wipe feature that was activated immediately after the incident and there is no reason to believe that the personal data was likely to have been accessed before such deletion took place; (c) the incident was reported without delay to the affected data subjects and it affects no more than 100 data subjects and it does not include sensitive personal data or personal financial data that could be used to carry out identity theft.

Even where there is no requirement to notify the loss to the Office, under the Code, the data controller must keep a record of each incident and the steps taken in response to it. This record is to be made available to the Office on request.

Data controllers who are obliged to report a loss of personal data to the Office must do so within two working days and must provide a detailed report of the incident to include:

- the amount and nature of the personal data that has been compromised;
- what action has been taken to secure and/or recover the personal data;
- what actions have been taken to inform those affected by the incident or reasons for the decision not to do so;
- what actions (if any) are being taken to limit damage or distress to those affected; and
- a chronology of events leading up to the disclosure.

Data controllers will also be required to furnish an additional report in which they describe the measures being undertaken to prevent repetition of the incident. The Office will investigate the issues surrounding the breach which may include on-site examination of the systems and procedures. The Data Protection Commissioner may also use his legal powers to compel certain actions which include requiring data controllers to inform data subjects about the security breach where they have not already done so.

Comments and observations on the Code should be sent to the Office before Friday 18<sup>th</sup> June 2010. Watch this space for further updates on this issue.



## Report of Data Protection Review Group on Breach Notification

Last month, the Minister for Justice, Equality and Law Reform, Mr. Dermot Ahern T.D. published the report from the Data Protection Review Group ("the Group") which examined whether legislative changes were required to address the issue of data breaches.

The Group concluded that a self-regulating regime (where organisations would decide for themselves whether or not to report data breaches) was not desirable or practical. It believed that the requirement to report breaches to data subjects was best moderated through reporting to the Data Protection Commissioner, as he already has powers to require organisations to inform data subjects of a data breach affecting them, under the Data Protection Acts 1988 and 2003. The Data Protection Commissioner can, if necessary, issue Enforcement Notices and failure to comply with such Notices is an offence.

The six recommendations of the Group are as follows:

1. Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in relation to the data protection principles - including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts for failure to comply with an Enforcement Notice issued by the Data Protection Commissioner - including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them.
2. The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice. This Code should be broadly based on the current guidelines from the Data Protection Commissioner, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the Data Protection Commissioner.
3. The Code should be reviewed on a regular basis by the Data Protection Commissioner and amendments submitted to the Minister as necessary to keep the legislation current.
4. The Data Protection Commissioner should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations which hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement.
5. Legislation should provide for the timely publication of the outcome of such audits, as an aid to good practice and in the interests of transparency.
6. The Data Protection Commissioner should continue to develop public awareness activities in this area.

As mentioned in another article in this TABS Update, following publication of the report, the Data Protection Commissioner published a Code of Practice specifying the circumstances in which the reporting of data breaches will be mandatory.

The Minister will consider the Group's recommendations in conjunction with data protection developments at EU level. It is likely that the review of the existing Data Protection Directive by the European Commission will give rise to a proposal for a new or amending Directive either later this year or during 2011 which will address many of the issues raised by the Group, including some form of mandatory notification to data subjects in cases of data breach.

In light of these developments, it is important that companies review their operations to ensure that the appropriate security measures and policies are in place to avoid a data breach occurring. As a breach will damage a company's reputation (and also have financial consequences), prevention is really better than the cure!

## Danone wins Supreme Court appeal

Compagnie Gervais Danone ("Danone"), the French food products company, has succeeded in its Supreme Court appeal against a High Court ruling. Danone issued legal proceedings against Glanbia Foods Society Limited ("Glanbia") in the High Court as it claimed that by using the brand name, YOPLAIT ESSENCE on a range of probiotic yoghurts, Glanbia had infringed its Irish registered trade mark, ESSENSIS. This was disputed by Glanbia who, in its Counterclaim, contended that the trade mark had not been used by Danone within the past five years and therefore should be revoked. Glanbia referred to the fact that Danone marketed yoghurt products under the trade marks, ACTIVIA and DANONE and that on the packaging for the ACTIVIA product, reference was made to the presence of an active ingredient called "Bifidus Essensis" which was a strain of bacterial culture aimed at aiding digestion. Glanbia claimed that ESSENSIS was not used on its own but was at all times used in conjunction with the word "Bifidus" to designate one of the ingredients of goods sold under the trade marks, ACTIVIA and DANONE.



In the High Court, Ms Justice Geoghegan found that the trade mark should be revoked on the grounds that it had not been put to genuine use in the State in relation to yoghurts (the goods for which the trade mark was registered) within five years since its registration was published. Having made certain findings of fact and having considered the relevant case law, Ms Justice Geoghegan did not believe that the use made of the trade mark, ESSENSIS was use as a trade mark in relation to yoghurts even though the trade mark was used on packaging and advertising materials. She found that use had been *“unequivocally confined to referring to an identified ingredient of the yoghurt as distinct from the yoghurt itself”* and concluded that such use was not use in accordance with the essential function of a trade mark in guaranteeing the identity of the origin of the yoghurt. As the trade mark was revoked, the infringement claim did not proceed. This decision was appealed by Danone.

Giving the (unanimous) judgment, Ms Justice Macken said that she was satisfied that Danone had *“established....sufficient facts as to use of the trade mark ESSENSIS upon which the learned High Court judge ought to have concluded that the use of that mark was genuine trade mark use in respect of the products for which it is registered, namely yoghurt, and that by reason of an unduly narrow application of the principles relating to trade mark use, as established by the European Court of Justice, the learned High Court judge misdirected herself in law on the application of the appropriate principles to the evidence established in the course of the hearing”*. Furthermore, as the case law of the European Court of Justice cited in the judgment provided a *“sufficiently clear basis on which to determine the sole issue for resolution in this appeal”*, Ms Justice Macken said that there was no requirement to refer any question to the European Court of Justice for its opinion. The Supreme Court therefore set aside the judgment of the High Court and made an order refusing Glanbia’s application for revocation of the ESSENSIS trade mark. The lesson for other companies is that they should review their registered trade marks to ensure that they are being put to genuine use in Ireland, otherwise they may be vulnerable to revocation. The time to act is now....before it is too late!

## Illegal Downloads – Take Three!

In past editions of TABS Update, we reported on the case instigated by a number of record companies (“the Record Companies”) against Eircom (the largest broadband ISP in Ireland) seeking orders restraining Eircom from infringing copyright in sound recordings owned by, or exclusively licensed to them by making copies available to the public. TAB Readers will recall that the case was ultimately settled. Under the settlement, the Record Companies will supply Eircom with the IP addresses of subscribers who illegally upload or download copyright protected works. Eircom will then contact the subscribers directly warning them about their activities, disconnecting those who ignore the warnings under a “three strikes and you are out” policy. The Record Companies also agreed to take steps to put similar agreements in place with other ISPs in Ireland.

The case was recently back before the High Court as the parties sought the court’s opinion on whether the process leading up to termination amounted to an interference with subscribers’ personal rights. This was necessary as the Data Protection Commissioner had expressed concerns particularly as to whether the Data Protection Acts 1988 and 2003 was an obstacle to implementing the settlement. In the High Court, Mr Justice Charleton ruled that the IP addresses of suspected illegal downloaders in the hands of the Record Companies did not constitute “personal data” such as required to comply with data protection legislation. He also ruled that Eircom’s processing of the personal data of suspected illegal downloaders (as proposed) did not amount to unwarranted processing that prejudiced the fundamental rights and freedoms or legitimate interests of subscribers.

Is this the end of the matter? No.....as the Record Companies have now gone after O2 and 3G, issuing legal proceedings against both companies in an effort to get them to cut off subscribers that illegally share copyright material online. TABS Readers will recall that legal proceedings have also been instituted by the Record Companies against UPC Communications Ireland Limited which has been listed for hearing by the Commercial Court on 17<sup>th</sup> June 2010. The Record Companies are also reportedly in discussions with Vodafone Ireland.

The graduated response is emerging as the music industry’s preferred response to illegal online sharing. However, can the Record Companies agree this approach with other ISPs in Ireland - watch this space for further updates.

### Contact:

**Maureen Daly – Partner and Head of Technology And Brands**  
**Beauchamps Solicitors**

Riverside Two, Sir John Rogerson’s Quay, Dublin 2

Tel +353 (1) 418 0600 Fax +353 (1) 418 0699

email [m.daly@beauchamps.ie](mailto:m.daly@beauchamps.ie) web [www.beauchamps.ie](http://www.beauchamps.ie)

This ezine is for general information purposes only and does not comprise legal advice on any particular matter. You should not rely on any of the material in this ezine without seeking appropriate legal or other professional advice. While every care has been taken in preparation of this ezine, we are not liable for any inaccuracies, errors, omissions or misleading information contained in it.