It is not what you say – it is what you do that counts:
Maintaining confidentiality of information under the EU Trade Secrets Directive

The EU Trade Secrets Directive (Directive (EU) 2016/943) came into force on 5 July 2016 and is to be implemented by EU Member States into their national law by 9 June 2018.

One of the requirements for information to qualify as a “trade secret” under the Directive is that “reasonable steps” have been taken to maintain its confidentiality. In this article we focus on what the taking of reasonable steps is likely to mean in practice.

Defining a trade secret

The Directive, like the recent US Defend Trade Secrets Act, takes its definition of a “trade secret” from Article 38 of the TRIPS Agreement. Article 2(1) of the Directive defines a “trade secret” (emphasis added) as:

“…information which meets all of the following requirements:

(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret;

(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.”

Reasonable steps

The Directive does not define what would constitute “reasonable steps”. However, the wording of the Directive is broadly in line with the way in which the law of confidential information and trade secrets has developed in the United Kingdom. Accordingly, the case law of England and Wales may provide some clues as to what will constitute “reasonable steps” under the Directive, namely: (1) telling people to keep information secret; (2) limiting access to that information; and (3) not simply relying on technical barriers to protect it.

1. Tell the recipient to keep information confidential - to create an obligation for the recipient to keep information confidential it must be shared by the holder in “circumstances importing an obligation of confidence” (See Coco v A.N. Clark (Engineers) Ltd [1968] FSR 415).

How?
This can be achieved in a number of ways including, for example, through the execution of confidentiality agreements where appropriate, incorporating confidentiality provisions into relevant agreements – such as employment contracts or supplier agreements - and marking documents containing trade secrets as “Confidential”.

T +44 20 7242 8692
F +44 20 7405 4166
E email@carpmaels.com
2. Keep access to confidential information on a strictly “need to know” basis – for information to qualify as a trade secret, the owner must have “limited or at least not encouraged or permitted widespread publication” (See Lansing Linde v Kerr [1991] 1 WLR 251).

How?
A practical way to address this is to develop and use a confidential information policy in your business which categorises the types of confidential information held by the business, specifies which members of staff can access that information (restricting access as necessary) and also sets out any restrictions that apply to the use of that information.

3. Do not rely on technological barriers – under the Directive, the acquisition of a third party’s trade secret will be considered lawful if it has been obtained through “observation, study, disassembly or testing” (e.g. reverse engineering) a publicly available product or object (provided whoever carried out the observation, study, disassembly or testing was not under any legal duty not to do so) (Article 3(1)(b)). Similarly, in England and Wales the courts have found that information obtained through reverse engineering may not be a breach of confidential information – if it is “easy to reverse engineer” (See Cray Valley Ltd v Deltech Europe Ltd [2003] EWHC 728 (Ch) as cited in Kerry Ingredients (UK) Ltd v Bakkavor Group Ltd & Ors [2016] EWHC 2448 (Ch)).

How?
Carefully consider what information (including information contained within products or objects) is placed into the public domain. To the extent possible, avoid putting into the public domain products or objects from which confidential information could be derived (particularly if it would be reasonably easy to reverse engineer). Also consider including contractual restrictions on the use of such products or objects. For example, one mechanism used frequently in respect of software is a contractual limitation on users preventing them from decompiling or reverse engineering the software.

Next steps
With 18 months to go until the Directive is implemented into the national law of Member States - now is the time to:
• ascertain what confidential information your business holds;
• audit and if necessary update your policies for protecting trade secrets; and
• check the contractual controls that you have in place – NDAs, employment agreements, customer agreements, and any contracts under which you will disclose confidential information.

Author: Chloe Taylor

Need advice?
For further information on confidentiality in the UK and/or the Directive you may wish to review our webinars on these topics. For more information, please contact: email@carpmaels.com.

If you have specific questions about your company’s approach to trade secrets, please contact one of the members of our Transactions Team.

Carpmaels & Ransford LLP is a leading firm of European patent attorneys based in London. For more information about our firm and our practice, please visit our website at: www.carpmaels.com.

This information provides a summary of the subject matter only.

It should not be acted on without first seeking professional advice.

Carpmaels & Ransford LLP is regulated by the Intellectual Property Regulation Board (IPREG).

Copyright © Carpmaels & Ransford LLP 2016