Innovation, the European market and the new EU Trade Secrets Directive
A new law for Europe

In 2015, Europe will, for the first time, have a single unified framework for protecting confidential business information. The Trade Secrets Directive will facilitate international business growth and create a single system of minimum protections across all 28 EU member states.

Without warning, on 28 November 2013, the European Commission (‘EC’) published a draft Trade Secrets Directive. Although those in the know were aware the EC was looking at the problems created by a lack of consistent protection for innovative ideas across Europe, and there had been some consultation, nobody was expecting the publication of a Directive so quickly.

Following additional consultation, an amended ‘compromise draft’ was published on 4 March 2014 by the Presidency, which was followed by a further version on 26 May 2014 from the Council. The European Parliament will now debate whether to pass the original draft or the latest compromise draft, or an altered version of one of them.

Although the Directive is expected to be passed before summer 2015 and for local laws to be passed during the two years which follow, many organisations are already planning to exploit the opportunities it creates.

The aim of the Directive is to harmonise the protection of trade secrets across the 28 member states of the EU. But why? The reason lies in the preamble to the Directive: the EC is concerned to ensure the smooth functioning of a single European market and as part of the ‘EU 2020 Strategy’ obligated itself to create an innovation-friendly environment for business.

Legislators are increasingly recognising that innovation is critical to the economies of industrialised nations. Intangible assets like trade secrets and confidential information have grown to account for approximately 80% of the market value of publicly traded companies, and businesses of all sizes depend on them for continued competitive advantage.

In a world where the US has had trade secret protection laws for several years but a third of EU states still have no trade secret legislation, the disadvantage to business in the European market is clear.
What will the Trade Secrets Directive do?

The Directive will harmonise laws across the EU in three main areas:

1. the definition of what is a ‘trade secret’, and the ways in which they will be protected throughout Europe;
2. the remedies available to trade secret holders when they suffer a theft or unauthorised use of their trade secrets; and
3. the measures the Court can use to prevent trade secrets leaking during legal proceedings.

The Commission’s approach, as explained in the memo accompanying the draft Directive, is that trade secrets are not in themselves intellectual property rights, although they often include information which could become protectable through established intellectual property rights in future. For example, experimental results can eventually form the basis of a patent application, but until that point will be protected by trade secrets laws. In future, it may therefore be more viable to elect not to patent an invention and to rely on trade secret protection instead.

It’s ‘secrecy’, but not as we know it

At the moment, there is an inconsistent level of protection of sensitive data across the EU member states. Only around two thirds of EU states currently have specific legislation concerning the misappropriation of trade secrets. The remaining countries, such as the UK, France and the Netherlands rely on a mixture of judicial interpretation of extra-contractual liability and traditional common law.

Even in countries where there is existing legislation, there may still be no statutory definition of what a trade secret is. Instead, definitions have mostly evolved through judicial interpretation of more general laws. This is true to an even greater extent in countries with common law legal systems, such as the UK.

In part, the inconsistency in the existing trade secrets regulation across the EU reflects the pervasive nature of trade secrets, as well as the fact that different countries have approached the issue from different starting points without any overarching co-ordination. For example, in France, there is legislation to protect against misappropriation of trade secrets in the employment relationship — but not in an intellectual property context (which instead relies on principles derived through case law). Likewise, in Germany, trade secrets are regulated through both competition law and employment law. To complicate things further, this also produces more than one definition of a trade secret in countries such as France, Germany and the UK, depending on whether the information is disclosed in the context of the employment relationship or not. This is clearly unhelpful for innovation in international businesses.

Certainty at last

When the Directive is implemented, businesses will have certainty for the first time that their sensitive or confidential information can be protected throughout Europe — as long as they make sure they keep it within the following definition:

1. that it is ‘secret’ in the sense that it is not generally known by, or readily accessible to, people in the wider community who normally deal with that kind of information. This applies not only to single pieces of information, but crucially to collections of information. This ensures that manuals, processes and recipes can all be protected, as long their precise configuration is not generally known outside the business or its contractual supply chain. It also means that it will become easier to enforce confidentiality over CRM data and software features and functionality across Europe; and
2. it has commercial value, not necessarily an intrinsic financial value, because it is ‘secret’; and
3. has been subject to reasonable steps to keep it ‘secret’ by those who lawfully hold the information. The means that as long as your supply chain, licencees, franchise holders and other business partners are required to observe your security requirements for the information, then it remains ‘secret’ and protectable.
New protections

Under Article 3 of the Directive, the use or disclosure of a trade secret will be unlawful whenever it is carried out without the consent of the trade secret holder by a person who has acquired the trade secret unlawfully through unauthorised access, copying or removal or through any other conduct which should be considered to be ‘contrary to honest commercial practices’.

Use or disclosure will also be unlawful where it occurs without consent and in breach of a confidentiality agreement or other duty not to disclose the information. This places some emphasis on businesses helping themselves by ensuring they have the correct contractual documentation with their employees and throughout the supply chain. Where a trade secret is obtained from a third party, the use or disclosure of it may still be unlawful if the person knew, or should have known, that the person from whom it was obtained was using or disclosing the trade secret unlawfully.

Businesses should also be reassured by Article 8 of the Directive, which will require member states to introduce measures necessary to preserve the confidentiality of trade secrets during legal proceedings. This includes, at least, the option to restrict parties’ access to documents and hearings and order them to be disclosed to/carried out in the presence of specific persons only. At the very least it will see ‘confidentiality clubs’ become more commonly used across Europe to control the dissemination of confidential evidence in trade secrets disputes. While these are common in the UK, there is currently no equivalent in a number of member states.

“The Directive does not provide remedies where an employee retains sensitive information after their employment ends.”

This definition corresponds closely to the existing definitions in some EU member states such as Denmark, Spain and Italy. Elsewhere, such as in the UK, Germany, Poland and Hungary, however, the requirement for a trade secret to have commercial value will narrow the existing definitions of confidential information. This raises an important question for member states: whether implementation of the Directive should come in addition to, or instead of, their existing laws.

In practice, it seems most likely that the implementation of the Directive will alter the practice of local courts so that the Directive protections are effectively extended to cover other types of confidential information. It would be unexpectedly perverse if the litigation adopted the procedural measures set out in the Directive, only for those protections to fall away if the information in question was found to fall outside the Directive definition of ‘trade secret’ during the litigation.

As an added bonus, the Directive’s approach is very similar to that of the US Uniform Trade Secrets Act, which defines a ‘trade secret’ as being that which:

1. derives independent actual or potential economic value from not being generally known to, or readily ascertainable by, other persons who can obtain economic value from its disclosure or use; and

2. is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

This similarity should further promote the confidence of transatlantic businesses to expand their operations in Europe.

One similarity that the EU will not share with the US, however, is criminalisation of trade secret misuse. Although some states, such as Germany, France and Finland, already have varying degrees of criminal sanctions in this area, the EU will not compel or encourage other member states to follow suit.
Insider threat

One area where the EC has deliberately left a gap, however, is in the treatment of employees. Due to a higher level concern that local employment laws should not be interfered with, the Directive does not provide remedies where an employee retains sensitive information after their employment ends. As long as an employee claims not to be ‘using’ the data, employers will have no specific protection under the Directive and therefore will need to rely on their contractual arrangements with employees to force them to return sensitive materials.

As a result, there is now a greater imperative than ever before for international organisations to take a harmonised and co-ordinated European approach to their employment contracts and rules around confidential materials.

A new asset class

An additional consequence of keeping any type of commercial information ‘secret’ in this way, particularly the ability to maintain legal ‘secrecy’ by a series of contractual measures with third parties, is that the information can become commercially exploitable in its own right. Some businesses are already exploring new charging structures based on their new ability to classify specific sets of data as ‘trade secrets’. There is clear potential for the exploitation of previously private processes, recipes or datasets in similar ways or through licensing or franchising.

New legal protections throughout Europe

Having ensured that they have implemented measures which satisfy the legal test of ‘reasonable steps... to keep it secret’, businesses will have a range of solutions available to them if valuable information does walk out the door with employees, contractors, LLP members, business partners or ex-franchisees. If a trade secret is used, copied or disclosed without permission by someone who has acquired it unlawfully, has broken a contract that limits its use (such as a licence or franchise agreement) or has breached a confidentiality agreement or NDA, then the remedies available to the trade secret holders include:

- Injunctions to prevent further use or disclosure of the information
- Court orders prohibiting infringing goods from being produced, marketed, sold, stored, imported or exported
- Seizure or delivery up of infringing goods (including imported goods) to stop them being circulated in the market
- Delivery up of electronic information, even where it is part of a larger file or materials
- Court orders compelling product recalls
- Orders requiring alteration to the products, so that infringing characteristics are removed. This includes software and electronic data, such as customer databases
- Destruction of infringing goods
- Publication of judgments in appropriate cases.

Use in this context also includes using the information to ‘significantly benefit’ the design, functioning or processes used in other products. Businesses are likely to have up to a maximum of six years to take action for damages, although it remains possible that the European Parliament will opt for a shorter maximum limitation period. It is appreciated that interim injunctions are often needed in trade secret breach cases and the Directive therefore specifically provides for them.

Through increased use of confidentiality agreements and updated commercial agreements, businesses will be able to begin to show they are taking ‘reasonable steps’ to keep information secret and open the door to new revenue and product lines. But documentation alone is not the whole answer. It needs to be accompanied by a series of practical measures, implemented in an integrated way through the collaboration of stakeholders such as the HR, Legal, Compliance and IP functions.

“In preparation for the new legal framework, it is now a good time to start to introduce measures to show that ‘reasonable steps’ are in place to protect manuals, processes, formulas, recipes, software and CRM data at all levels.”
What does all this mean for industry?

The Directive undoubtedly creates new protections and opportunities. Apart from increasing the range of protective steps available across Europe and increased business certainty, both the exploitation of new product lines and increased leverage from existing products are now definitely possible.

The key to ensuring your organisation can take advantage of these possibilities will lie in satisfying the two core elements of the ‘trade secrets’ definition: that it stays ‘secret’ as described above and is subject to reasonable steps to keep it ‘secret’ throughout the supply chain.

In preparation for the new legal framework, it is now a good time to start to introduce measures to show that ‘reasonable steps’ are in place to protect manuals, processes, formulas, recipes, software and CRM data at all levels. Security arrangements should be reviewed and updated to ensure that effective and consistent measures are implemented all the way from employees, contractors and freelancers through to suppliers and franchisees.

Measures should range from making sure that documents are appropriately marked as ‘confidential’ to pre-employment vetting of R&D staff and physical and electronic segregation of the information you need to protect. Alongside this, contractual confidentiality and security obligations also need to be updated and applied consistently across business units and jurisdictions.

Getting these steps right should ensure that your business is well set to take advantage of the new international legal framework with additional confidence.

For more information on protecting or exploiting your trade secrets, please contact:

**Warren Wayne**
Tel: +44 (0)20 7905 6230
warren.wayne@twobirds.com

**Robert Williams**
Tel: +44 (0)20 7415 6089
robert.williams@twobirds.com

Alternatively, please contact the relevant individual/s from your country from the list of names overleaf.

“Some businesses are already exploring new charging structures based on their new ability to classify specific sets of data as ‘trade secrets’.”
Key contacts

International Trade Secrets Protection group co-heads:

**UK**
Warren Wayne  
warren.wayne@twobirds.com  
Robert Williams  
robert.williams@twobirds.com

International Trade Secrets Protection group contacts:

**Belgium**
Christophe Delmarcelle  
christophe.delmarcelle@twobirds.com  
Bruno Vandermeulen  
bruno.vandermeulen@twobirds.com

**China**
Christine Yiu  
christine.yiu@twobirds.com

**Czech Republic**
Vojtech Chloupek  
vojtech.chloupek@twobirds.com  
Michal Dejmek  
michal.dejmek@twobirds.com

**Denmark**
Peter Lind Nielsen  
peter.nielsen@twobirds.com  
Søren Narv Pedersen  
soren.pedersen@twobirds.com

**Finland**
Maija Nikkola  
maija.nikkola@twobirds.com  
Tom Vapaavuori  
tom.vapaavuori@twobirds.com

**France**
Rebecca Delorey  
rebecca.delorey@twobirds.com  
Benjamine Fiedler  
benjamine.fiedler@twobirds.com

**Germany**
Matthias Meyer  
matthias.meyer@twobirds.com  
Martin Nebeling  
martin.nebeling@twobirds.com

**Hong Kong**
Richard Keady  
richard.keady@twobirds.com  
Padraig Walsh  
padraig.walsh@twobirds.com

**Hungary**
Bálint Halász  
balint.halasz@twobirds.com  
Zoltan Tarjan  
zoltan.tarjan@twobirds.com

**Italy**
Giovanni Galimberti  
giovanni.galimberti@twobirds.com  
Caterina Rucci  
caterina.rucci@twobirds.com

**Netherlands**
Philip Hartman  
philip.hartman@twobirds.com  
Wouter Pors  
wouter.pors@twobirds.com

**Poland**
Maciej Gawroński  
maciej.gawrons@twobirds.com  
Karolina Stawicka  
karolina.stawicka@twobirds.com

**Singapore**
Chia Ling Koh  
chialing.koh@twobirds.com  
Kavitha Rajan  
kavitha.rajan@twobirds.com

**Spain**
Manuel Lobato  
manuel.lobato@twobirds.com  
Miguel Pastur  
miguel.pastur@twobirds.com

**Sweden**
Katarina Åhlberg  
katarina.ahlberg@twobirds.com  
Gabriel Lidman  
gabriel.lidman@twobirds.com

twobirds.com/tradesecrets