ICLG

The International Comparative Legal Guide to:

Patents 2016

6th Edition

A practical cross-border insight into patents law

Published by Global Legal Group, in association with CDR, with contributions from:

AAA Law
Adams & Adams
AEQUO
Anderson Mori & Tomotsune
Armengaud & Guerlain
Beuchat, Barros & Pfenniger
Bird & Bird LLP
Cabinet Enpora Intellectual Property
Carroll, Burdick & McDonough LLP
Daniel Advogados
DELACOUR
Fiebinger Polak Leon Attorneys-at-Law
Gorodissky & Partners
Griffith Hack Lawyers
Gün + Partners
Jackson, Etti & Edu
JMB DAVIS BEN-DAVID
Kadasa & Partners
Kirkland & Ellis LLP
LAW OFFICE POPOVIĆ, POPOVIĆ, SAMARDŽIJA & POPOVIĆ
OLIVARES
Patentbureau Paul Rosenich Inc
Patrinos & Kilimiris
Perry + Currier Inc.
Pham & Associates
REIMANN OSTERRIETH KÖHLER HAFT
Rouse & Co. International
Spence PC
Subramaniam & Associates
SyCip Salazar Hernandez & Gatmaitan
Synch Advokat AB
Tilleke & Gibbins
TIPLO Attorneys-at-Law
Wikborg Rein
Whitney Moore Solicitors

CDR Commercial Dispute Resolution
GLG Global Legal Group

The Trade Secrets Directive – Harmonisation of Trade Secrets Law in the EU is on the Way

Robert Williams

Warren Wayne

Bird & Bird LLP

Introduction

On 28 November 2013, the European Commission ("EC") published a draft Trade Secrets Directive (the "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 stakeholder and public consultation, the publication of a Directive so quickly came as a surprise to many.

A period of consultation followed, during which a number of fairly fundamental points were raised, and an amended "compromise draft" was published on 4 March 2014 by the Presidency (followed by a further version, on 26 May 2014[1] from the Council). Since then, the draft has been passed on to the European Parliament (at the end of 2014), where it is being considered by the Committee on Legal Affairs (JURI). The process has slowed down a bit since then, although some other committees in the Parliament have been feeding their opinions to JURI in the meantime[2]. The next formal step in the process is a plenary hearing in the Parliament, which has been scheduled for 8 September 2015, although prior to that it is anticipated that JURI will adopt (and publish) a draft Report on the proposal.

Accordingly, the Directive still has a little way to go before it is "finalised", and whilst numerous stakeholder views have been considered (and taken account of) during the Commission/Council phase, it remains to be seen precisely how it will turn out following its passage through the Parliament. It is hoped that it will be passed by early 2016, following which local laws will then need to be enacted during the following two years in order to bring its provisions into force across the EU.

Whilst this is still a little way off, many organisations are already considering how the Directive may affect them and planning to exploit the opportunities it creates. In this chapter we will look at a number of the key issues covered in the Directive, focusing on the 26 May 2014 version (which has received the most consideration and commentary) for this purpose.

Background

The aim of the Directive is to harmonise the protection of trade secrets, across the 28 Member States of the EU. 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[3].

Legislators are increasingly recognising that innovation is critical to the economies of industrialised nations. Intangible assets 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.

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 the future. In particular, trade secrets go hand in hand with patents – for example, experimental results can eventually form the basis of a patent application, but until that point will be protected by trade secrets laws. Additionally, in certain circumstances it is more viable to elect not to patent an invention and to rely on trade secret protection instead. This is something that may become a more attractive option when the Directive comes into force.

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.

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 coordination.

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, the UK and Germany, 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 should have certainty for the first time that their sensitive or confidential information can be protected throughout Europe. The definition of a Trade Secret proposed by the Commission is identical to that contained in the TRIPs Agreement definition of "undisclosed information", and is well known (at least at a conceptual level) in many countries. To be protected under this definition requires the following[4]:

1. that the information in question 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 customer service data and software features and functionality across Europe;
2. it has commercial value because it is "secret". This does necessarily mean that an intrinsic financial value has to be demonstrated; and
3. it has been subject to reasonable steps to keep it "secret" by those who lawfully hold the information[5].

This means that as long as a business's supply chain, licensees, franchise holders and other business partners are required to observe its security requirements for the information, then it remains "secret" and protectable.

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 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 for international companies, 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.

Whilst the Directive definition isn't finalised yet, it is anticipated that it will be sufficiently similar to the US Uniform Trade Secrets Act that this should further promote the confidence of international businesses to expand their operations in Europe.

One similarity that the EU will not share with the USA, 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 Member States to follow suit[6].

New Protections

Under Article 3 of the proposed draft 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 though unauthorised access, copying or removal or through any other conduct which should be considered to be "contrary to honest commercial practices". It has been suggested, however, that the Court of Justice of the EU will need to provide an independent interpretation of what "honest commercial practices" means in this context, before the Directive can be applied consistently across all Member States[7].

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 or carried out in the presence of specific persons only. At the very least it would see "confidentiality clubs" become more commonly used across Europe to control the dissemination of confidential evidence in trade secrets disputes. A "confidentiality club" is an agreement made by parties in litigation which limits access to confidential documents, so that they are only available to specified people. This helps to maintain the confidentiality of information, while permitting the parties to comply with their obligations to disclose evidence in the proceedings. While these are common in the UK, there is currently no equivalent in a number of Member States.

Insider Threat

Employees and contractors can be a particular threat to trade secret security, even if they are not malicious. Despite this, one of the areas where the EC has deliberately left a gap in the Directive is in the treatment of employees. Due to a higher level concern that local employment laws should not be interfered with, the Directive currently 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 need to rely on their contractual arrangements with employees to force them to return sensitive materials.

Even where employees have deliberately taken trade secrets, the EU Council has proposed a looser regime in comparison to other cases of unlawful trade secret acquisition: "*Member States should be able to establish a more favourable regime to employees in their liability for damages in case of unlawful acquisition, use or disclosure of a trade secret*"[8]. The corresponding amendment to Article 13(1) gives Member States the option of effectively forcing employers to prove intent in employee cases in order to recover damages. If that is adopted, it will reduce the effectiveness of the Directive to properly compensate businesses in cases of employee trade secret theft[9]. This will compel employers to rely more on the employee contract to ensure they are properly protected.

As a result of all these factors, there is now a greater imperative than ever before for international organisations to take a harmonised and coordinated European approach to their employment contracts and restrictions concerning the use of 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 Non-Disclosure Agreement, then the remedies include[10]:

- 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 groups. As a very significant amount of trade secret theft is carried out by staff or supply chain employees, the threat requires a broader approach.

There are currently no planned remedies in cases of reverse engineering, however. This is a concern in some industries, as highlighted by the Max Planck Institute: "*…the use without restrictions of trade secrets obtained through reverse engineering appears problematic, in particular in sectors where…considerable investments are made in the development of new products. Notable examples include the cosmetic industry, which regularly invests quite heavily in the development of perfumes, but where the know-how generated thereby can be decoded with relative ease through reverse engineering. The unrestricted use of such know-how raises concerns that it could pose a substantial threat to the companies concerned, eventually leading to market failure whereby such goods would no longer be produced.*"[11]

What Does This All Mean for Companies Now (and in the Future)?

The Directive will undoubtedly create new protections and opportunities for innovative companies that are operating in the EU, or entering it for the first time. 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 will now definitely be possible in the future.

The key to ensuring your organisation can take advantage of these possibilities will lay 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. This is not always taken seriously by international businesses, however, as discovered by PwC: "*Previous PwC surveys support the view that the supply chain is a potential weak link in cybersecurity – both in the United States and globally…Companies often struggle to get their suppliers to comply with privacy policies – a baseline indicator of data protection capabilities*."[12]

In preparation for the new legal framework, it is now a good time to introduce measures (if this hasn't already been actioned) to show that "reasonable steps" are in place to protect processes, formulas, recipes, manuals, software and CRM data at all levels:

- Security arrangements across Europe 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.
- Contractual confidentiality and security obligations with staff and throughout the supply chain 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 international legal framework with additional confidence.

Endnotes

1. EC 9870/14.
2. In particular, it should be noted that the Committee on Internal Market and Consumer Protection (IMCO) and the Committee on Industry, Research and Energy (IRE) have each submitted an opinion to JURI (on 30 March and 29 April 2015, respectively) which propose a number of amendments to the draft, some of which are quite significant. It remains to be seen, however, how many of these are taken in.
3. EC 9870/14, Section I, paragraph 2.
4. EC 9870/14, Article 2.
5. The IRE Opinion goes even further and proposes that the steps should be verifiable by the Court, making it even more important for the steps to be well documented.
6. EC 9870/14, Section II, paragraph 6: "*Member States agreed that the draft directive should not interfere with their national prerogatives regarding criminal law*."
7. Comments of the Max Planck Institute for Innovation and Competition of 3 June 2014 on the Proposal of the European Commission for a Directive on the protection of undisclosed know how and business information (trade secrets) against their unlawful acquisition, use and disclosure of 28 November 2013, COM(2013) 813 final.
8. EC 9870/14, Section II, paragraph 6 and Article 13(1).
9. It should also be noted that both the IRE and IMCO Opinions submitted to JURI to date contain proposals to amend the draft to strengthen the position of employees.
10. EC 9870/14, Articles 11 to 14.
11. See Endnote 7.
12. "Key Findings from the 2013 US State of Cybercrime Survey", PwC, June 2013.

Robert Williams
Bird & Bird LLP
15 Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 7415 6000
Fax: +44 7415 6111
Email: robert.williams@twobirds.com
URL: www.twobirds.com

Rob Williams is a partner and co-head of Bird & Bird's Intellectual Property Group in London. He also jointly leads Bird & Bird's International Trade Secrets Protection Group.

He has significant experience in both contentious and non-contentious IP work, advising on the full range of issues relating to patents, copyright, trade marks, designs and trade secrets/confidential information.

Rob has particular experience of complex IP disputes (with a focus on multi-jurisdictional patent litigation and trade secrets disputes) and has advised clients from a range of IP rich industries, including life sciences, energy and utilities, speciality chemicals, mechanical engineering and electronics on various strategic IP issues including lifecycle management.

Warren Wayne
Bird & Bird LLP
15 Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 7415 6000
Fax: +44 7415 6111
Email: warren.wayne@twobirds.com
URL: www.twobirds.com

Warren Wayne is a partner in the firm's Employment Group in London and is known for his work in the technology and financial services sectors. He also jointly leads Bird & Bird's International Trade Secrets Protection Group.

Specialising in a range of employment issues, Warren has particular experience in dealing with complex and high value disputes, drafting and litigating confidentiality issues and employment restrictions, software theft and ownership disputes, international restructures and acquisitions, executive severances, discrimination disputes, data protection issues and complex Employment Tribunal claims.

Warren regularly speaks on employment law and trade secret topics and appears on BBC Radio and Television news programmes.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk