IPR Helpdesk

Fact Sheet

July 2012

How to manage confidential business information

TABLE OF CONTENTS

Introduction

In today's competitive market, companies need to be as innovative as possible to prosper in the business environment and to keep the pace with progress. To this end, the development and acquisition of useful information is crucial to create and provide new and improved goods and services. Information about technology that makes a company's product unique, prototypes, or a list of key customers are just a few examples of business information. As the latter can therefore have a great commercial value and significant importance for the company concerned, its uncontrolled disclosure might potentially lead to serious consequences.

Small and medium-sized enterprises (SMEs) in particular may not be aware of this risk and thus of the importance of keeping this valuable information "confidential". Indeed, such information relates to intangible assets and falls under the category of intellectual capital, but its protection is not regulated within the intellectual property rights (IPR) system. That is why confidential information belongs to the so-called **Soft IP**.

The European IPR Helpdesk is managed by the European Commission's Executive Agency for Competitiveness and Innovation (EACI), with policy guidance provided by the European Commission's Enterprise & Industry Directorate-General.

European Commission

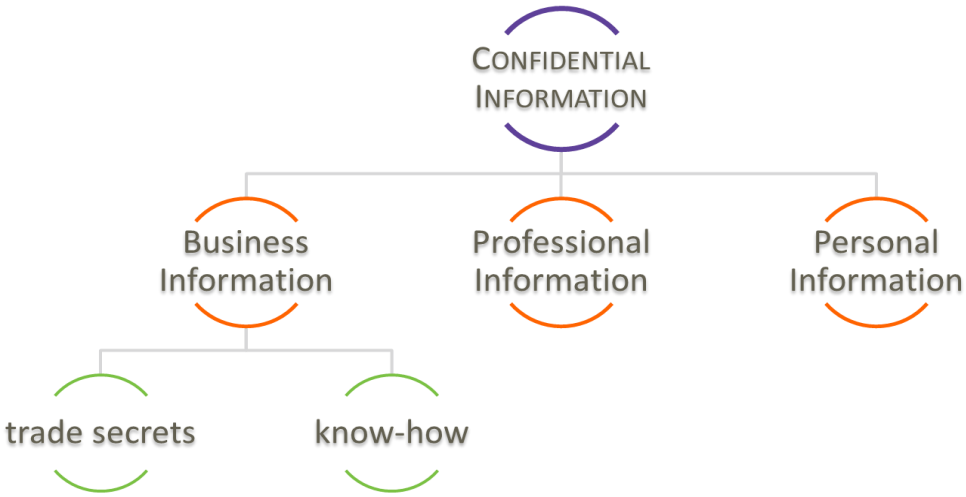
The present fact sheet will illustrate the importance of confidentiality for businesses and give hints on protection management of confidential business information, which could prove beneficial in particular to small and micro entities.

1. Confidential information and trade secrets

Confidential information is considered as information that must be kept secret. While any information can be confidential, not all the information generated within a company must be kept secret. What is confidential is then judged by the company on the circumstances of each individual case, based on the necessity of it not being disclosed.

Confidential information may refer to **personal information** (e.g. journals, pictures), **professional information** (e.g. information supplied in the course of professional duties) and **information in the context of business, commerce** or **trade** (i.e. trade secrets).

For the purpose of this document, we will focus on **trade secrets.** As it can be seen from the below diagram, trade secrets are confidential information related to the business and can be somewhat synonymous with **know-how**[1]. In practice however all these terms are often used interchangeably.



Broadly speaking, *trade secrets are any confidential business information which provides an enterprise with an economic benefit that translates into competitive advantage*[2], and this directly derives from the fact that the secret is generally unknown to competitors due to the efforts of its owner to keep it secret. In this sense, protection of trade secrets give incentive to innovate by safeguarding the substantial time and capital invested to develop innovations.

[1] Although know-how does not necessarily require secrecy, it acquires trade-secret status only if it is secret and has economic value and if measures are in place to secure its secrecy. Know-how becomes IP and is protected only if it qualifies as a trade secret.

[2] Some of the most common trade secrets are the Coca-Cola recipe, the Google algorithm and the New York Times Best Seller List. Although they are now large companies they started as SMEs and it is thanks to such trade secrets that they have become successful.

They are critical to the functioning of a company and any unauthorised or accidental disclosure of trade secrets may destroy their confidential status and may cause a considerable economic loss for the business[3] concerned. If not protected, competitors could use this information without having to bear the costs or risks and the owner of the trade secret would certainly lose the competitiveness built on this information. Trade secrets are relevant for example when a product or process is not considered worth a patent or is not patentable at all, as well as an alternative option to patenting[4]. Yet, they also play a fundamental role before seeking a patent. During this period in fact, disclosure of patent features may destroy patentability.

Given its non-material nature and economic value, all this information belongs to a company's intangible assets. However, **since trade secrets are a peculiar form of intellectual property (IP)[5], they require an appropriate internal management programme.** Any entrepreneur should put in place a safeguard system within its company for protection of trade secrets to be effective. This would require **goodwill** and **maintenance[6],** which in some cases is the most fruitful IP protection.

Indeed, a trade secret offers a **broader scope of protection** than other forms of IPR as, once the very low requirements are met, any information related to technology, design, art, marketing, idea, concept and so forth, can be protected. Moreover, trade secrets are **much cheaper** than IPR as they need no registration or any official procedure to be protected and, most importantly, as long as secrecy is kept they are **effective without time limits**. Therefore, the term of protection can be perpetual as regards trade secrets.

2. How to assess a trade secret

For information to be legally protected as a trade secret it must:

- ✓ Be unknown to the business circles that normally deal with that kind of information;
- ✓ Confer some sort of economic benefit because it is secret;
- ✓ Be the result of reasonable efforts to maintain its secrecy.

[3] An interesting case related to Ford Motor Co. An engineer of the company copied thousands of Ford's documents onto an external drive and went to work for a competitor. It was estimated that Ford suffered more than $50 million in losses.

[4] There can be some circumstances that may justify avoiding a patent. As an example, you offer a financial consulting service based on an evaluation market method. If you patented this method, competitors would be likely to revers it without any trace of infringement. In that case you will lose your competitiveness, thing that would not happen if you keep the method as a trade secret.

[5] Confidential information is not "property" like other forms of IP. Nevertheless, the Court of Justice of the European Union in its Microsoft judgment, Case T-201/04, and the European Commission in its Regulation 772/2004, Article 1.1.g, have stated that *trade secrets should be treated as equivalent to intellectual property rights*.

[6] Practical examples of measures that should be considered to protect a company's trade secret are provided in paragraph 4 of this fact sheet.

Some information qualifying as a trade secret:

- Information relating to formulas, patterns, devices or other compilation of information that is used for a considerable period of time in a business *(e.g. Coca-Cola recipe)*;
- Technical information used in the manufacturing process for production of goods, including software used for various business purposes *(e.g. the ZARA's IT system to shorten the production cycle)*;
- Marketing, export or sales strategies, or a method of bookkeeping or other business management routines or procedures *(e.g. list of key suppliers and/or buyers)*.

Other information may include financial information (e.g. business plans), purchase prices *of key raw materials, list of key customers, product specifications, test data, technical drawings or sketches, engineering specifications, contents of workbooks*[7]*, the salary structure of a company, any kind of agreement, promotional or marketing material under development*, and the like.

3. Forms of protection

Trade secrets do not confer apposite "proprietary rights", as it is the case with other IPR. Although at national level there is a long standing tradition of trade secrets protection (e.g. Italy, Germany, Bulgaria, France and UK), in the EU there is no harmonisation[8]. As a general rule, trade secrets are protected under **obligation of confidence** and their theft is considered **unfair trade practice**.

Obligation of confidence arises when an agreement has been reached between parties to maintain the information confidential. This can be done by the signature of a **Non-Disclosure Agreement** (NDA) or the insertion of **confidentiality clauses** within a contract. In both cases, the disclosure of the trade secret at stake would amount to a **breach of confidentiality** or **breach of contract,** which means that the recipient of that business information has used it without authorisation and in an unlawful way.

Differently from the breach of confidence where information has been "stolen" by someone having an obligation of confidence and a lawful access to it *(internal theft)*, **unfair trade practices** occur when the **misappropriation** of a trade secret is done by a third party (e.g. **competitors**) having no contractual obligation *(external theft)* and realising acts of **theft, espionage,** or **corruption of employees** (**bribery**). Such acts are generally treated under **unfair competition laws**.

[7] Workbooks stand for laboratory books or log books especially suitable for the IP generated in R&D projects.
[8] At international level only a minimal legal standard for their protection is provided; *see* Agreement on the Trade Related Aspects of Intellectual Property Rights (TRIPS), protection of undisclosed information, Article 39 (2).

3.1. Remedies

Civil remedies arising from these forms of liability are usually allowed. Depending on the national laws the owner of the trade secret may be entitled to:

- An injunction restraining the further use or disclosure of the information;
- An order allowing the search of premises and seizure of documents and products[9];
- Monetary compensation based on damages, loss of profits, unjust enrichment.

In order to **establish violation** of trade secrets, businesses should in principle show:

- The breach of confidentiality or the gain of competitive advantage by the person/company which has misappropriated the trade secret;
- That all reasonable steps to maintain the information as a trade secret have been taken;
- That there is misuse of the information concerned[10].

It is worth noting that businesses are protected from the mere unauthorised and unlawful disclosure and use of their trade secrets. This means that the **disclosing party cannot be deemed to be responsible** for breach of confidence, nor for unfair practice if the information:

- Was disclosed accidentally;
- Was acquired fortuitously;
- Was unlawfully passed on without any knowledge of its illegality.

Only voluntary acts constitute trade secrets infringement and may convey liability to the executor.

Many EU Member States have criminal sanctions (including imprisonment and fines) against trade secret's misuse. Imprisonment in some of these countries can go up to eight years and there are examples of criminal convictions[11].

4. Trade secrets protection management

Trade secrets misappropriation can be extremely damaging with severe consequences for the business, such as financial losses. Any company is vulnerable to theft of its business-critical information and should consequently take measures and implement a range of best practices to maintain confidentiality.

[9] This can be ordered in the case where there is a risk that evidence may be destroyed.
[10] The trade secret has been used or disclosed in violation of honest commercial practices.
[11] For example in Austria a former employee of the American Superconductor Corporation was sent one year to jail (and sentenced further two years of probation) for selling confidential information to a Chinese company.

4.1. Identification of trade secrets

To start with, a strategic assessment of a company's valuable business information is a prerequisite to set a protection programme. To identify trade secrets, two fundamental questions should be asked:

- ✓ **Does the information bring any economic benefit to my business?**
- ✓ **Would its leak hurt my business?**

Making a list of all this information and organising it into different sections, depending on its value to the business, will help understand the type of measures to take for its protection to be effective.

4.1.1. Protection policy

This would be part of a broader process which incorporates the company's **trade secret policy**. That is, once a company has evaluated that its business activity relies on an amount of valuable know-how, it should set a protection policy[12] to provide clarity (particularly to its employees) on all the aspects that need to be addressed.

The policy should explain why information should be kept confidential and how to do so. In the latter case, it should be explicit on the means used by the company to keep confidentiality, such as administrative, physical and technical controls. It is very important to define how information should be revealed and how it can be shared within and outside the business premises. It is also advisable to provide a list of the information not covered by confidentiality.

All the above is essential to protect the information assets from disclosure to any person not authorised to have access to them and would furthermore help those under obligation of confidentiality to understand when and to who it is possible to disclose information.

4.2. Store confidential information safely

Perhaps the most important aspect of a protection management programme is to securely store trade secrets in places where access is allowed under authorisation, such as *archives, safes or other appropriate locked rooms*[13]. Only personnel needing to know it should have access to the information.

Electronically stored information should be technologically protected. At least two security measures should be executed:

- ✓ **Use of passwords to access the system, and regular change of passwords;**
- ✓ **Automated control to enable system security personnel to trace any additions or changes back to the originator.**

[12] It is advisable to distribute a written information security policy at the hiring phase.

[13] In the Coca-Cola recipe case for example, the written version of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, and that vault can only be opened by a resolution from the company's Board of Directors. It is the company's policy that only two persons in the company must know the formula.

Besides that, take into consideration the use of up-to-date operating systems, anti-virus and anti-spyware software, to regularly back up information stored on hard drives and to store the backup media in the above-mentioned locked facilities.

4.3. Employee awareness

To avoid your business strategy being disrupted, employees should be aware of the company's security policy and their duty with regard to confidentiality, as well as the consequences of a breach of such duty.

4.3.1. Employee training

Employee education is then fundamental to handling trade secrets as they are meant to be used in business activities. Training on information security allows the establishment of a culture of information security within the organisation and is perhaps the most profitable aspect of confidentiality management.

4.3.2. Non-disclosure clauses

Although in most EU countries it is not necessary to sign a separate confidentiality agreement due to the national labour laws that require a confidentiality duty on the employees, it is highly recommended that strong contractual provisions be foreseen. This is the case of **non-disclosure clauses** within employment contracts[14] that oblige employees not to use trade secrets acquired in the course of the employment.

Confidentiality clauses should clearly state:

- **The business information to which the obligations apply;**
- **The specific obligations and restrictions imposed on the recipient;**
- **The consequences of breach of confidentiality;**
- **The obligations to be applied after termination of their employment with the organisation.**

4.3.3. Non-compete agreements

Employees leaving the company are a source of expertise (i.e. knowledge, skills, and experience) acquired therein. While the latter cannot be restricted, signing **non-compete agreements**[15] would ensure that trade secrets acquired during the employees' duties are safeguarded for a certain period of time after their departure. More precisely, these agreements would require a former employee not to work for a direct competitor up to the time when the secret information loses its inherent value to the business[16].

4.3.4. Employee activity monitoring

Another viable practice is to **monitor employees' activities**. In this sense, it is possible to conduct information security audits, thus monitoring the compliance of present employees with the

[14] If you need assistance, the European IPR Helpdesk can revise the part concerning confidentiality clauses within employment contracts.

[15] This can be done also in the form of non-compete clauses to be included within employment contracts.

[16] Depending on the value of the information, the terms of a non-compete agreement should be reasonable. The common practice is generally a **one-year time** restriction.

confidentiality rules and pursuing departing employees who have breached their obligation. It is also advisable to interview employees leaving the company to remind them about their confidentiality duty.

4.3.5. Document marking

Although employees are under a confidentiality obligation**, marking documents** can prove to be crucial by allowing employees to properly treat the documentation, avoiding incurring liability, and mainly by making sure that information are handled in a confidential manner.

There are different ways for marking trade secret information. Some of them are:

- CONFIDENTIAL
- THIRD PARTY CONFIDENTIAL
- MAKE NO COPIES
- DISTRIBUTION LIMITED TO ____
- COVERED BY A NON-DISCLOSURE AGREEMENT

Each of them can be further classified as CRITICAL, MAXIMUM, MEDIUM, and MINIMUM

4.4. Business partner commitment

4.4.1. Non-disclosure Agreements (NDA)

When revealing sensitive business information to a partner, the fact of simply attaching a confidentiality notice to the communication does not automatically create an obligation on the receiving party. The best approach to keep confidential business information away from competitors is indeed to make your business partners sign a Non-disclosure agreement (NDA)[17]. Thanks to these contracts, the recipient will be impeded in disclosing trade secrets and if a disclosure occurred, it would be liable to breach of contract and likely to be subject to financial penalties.

Since business information may represent a dominant factor in making prospective partners decide whether to start a new business relationship[18], NDAs are extremely useful before disclosing any valuable information related to the business during partnership negotiations such as licensing and joint ventures.

[17] For further information about NDAs, see the European IPR Helpdesk fact sheet "Non-Disclosure Agreement: a business tool", available in the library section of our website. The European IPR Helpdesk has also prepared NDA templates to assist you in case you are drafting your own contract. Templates can be found in the library section, within the useful documents box. In case you need tailored assistance, our Helpline can also analyse your agreement within three working days.

[18] To have a better overview on the issues that need to be discussed in an IP negotiation, see the European IPR Helpdesk fact sheet "How to deal with IP-related issues in transnational negotiations", available in the library section of our website.

4.4.2. Licences and joint ventures

Once the business relationship is set, non-disclosure contractual clauses should then be included in licence and joint venture arrangements.

As with confidentiality provisions in employment contracts, licence and joint venture agreements overall should also state:

- **The business information to which the obligations apply;**
- **The specific obligations and restrictions imposed on the recipient;**
- **The consequences of breach of confidentiality;**
- **The obligations to be applied after termination of the business relationship.**

Within *licence agreements*, besides explicitly and clearly foreseeing the duty of confidence, conditions on how and when to use the trade secret can be defined.

Regarding *joint venture agreements*, they should regulate two layers of confidential information, namely the trade secrets brought by partners before the venture and those that are the result of the venture. Accordingly, contractual clauses should define the ownership and protection of trade secrets during and after the joint venture.

4.4.3. Document marking

Although marking the relevant correspondence with your partners as confidential is not per se sufficient to make it binding to confidentiality obligations, as with internal correspondence it is strongly advisable to mark trade secret information with external parties[19].

5. Limits of trade secrets

Although trade secrets are an outstanding resource for a company's competitive edge, there are some drawbacks that need to be taken into consideration when developing an IP strategy.

Firstly, a trade secret can be reverse-engineered[20] and then competitors can commercialise the same or even more innovative product or process. As already mentioned, trade secrets only protect against unlawful acquisition and use of the confidential information. Furthermore, since there is no formal protection tool provided by the IP system, anyone may patent the invention covered by the trade secret if this has been developed by legitimate means.

Besides other features pointed out within the text, here below there is a table showing the relationship between patents and trade secrets:

[19] *See* above paragraph 4.3.5.

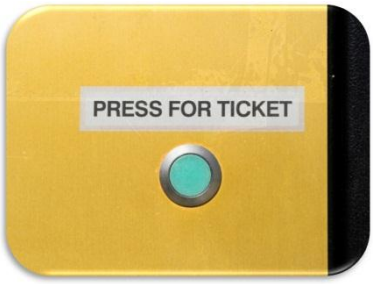
[20] Reverse engineering occurs when a trade secret is discovered lawfully by simply using the information publically available.

	Pros	Cons
Patents	• Monopoly / Exclusive rights • Court actions • Base for loans • Involuntary infringement	• High costs • 20 years limited protection • Disclosure • Length of procedures
Trade Secrets	• No registration costs • Not limited in time • No disclosure required • Immediate effect	• Not easily enforceable • Voluntary infringement • Can be patented by others • Limited remedies

Useful Resources

- *Roadmap for Intellectual Property Protection in Europe, Trade Secret Protection in Europe, which is part of a series of guides prepared under the EU-China Project on the Protection of Intellectual Property Rights (IPR2), available at* http://ipr2.org/document-centre/document.php?id=191#
- *WIPO IP Panorama e-learning module 04 on Trade Secrets, available at* http://www.wipo.int/sme/en/multimedia/
- *Fact sheet on "Non-Disclosure Agreement: a business tool":* http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Non%20Disclosure%20Agreement.pdf
- *Mutual Non-Disclosure Agreement – European IPR Helpdesk Template:* http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/NDA%20European%20IPR%20Helpdesk.pdf
- *One-way Non-Disclosure Agreement – European IPR Helpdesk Template*: http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/1WayNDA%20European%20IPR%20Helpdesk.pdf
- *Fact sheet on "How to deal with IP-related issues in transnational negotiations":* http://www.iprhelpdesk.eu/sites/default/files/newsdocuments/How_to_deal_with_IP_issues_in_transnational_negotiations_0.pdf

GET IN TOUCH



©istockphoto.com/Dave White

For comments, suggestions or further information, please contact

European IPR Helpdesk

c/o infeurope S.A.

62, rue Charles Martel

L-2134, Luxembourg

ABOUT THE EUROPEAN IPR HELPDESK

The European IPR Helpdesk aims at raising awareness of Intellectual Property (IP) and Intellectual Property Rights (IPR) by providing information, direct advice and training on IP and IPR matters to current and potential participants of EU funded projects focusing on RTD and CIP. In addition, the European IPR Helpdesk provides IP support to EU SMEs negotiating or concluding transnational partnership agreements, especially through the Enterprise Europe Network. All services provided are free of charge.

Helpline: The Helpline service answers your IP queries within three working days. Please contact us via registration on our website (www.iprhelpdesk.eu), phone or fax.

Website: On our website you can find extensive information and helpful documents on different aspects of IPR and IP management, especially with regard to specific IP questions in the context of EU funded programmes.

Newsletter & Bulletin: Keep track of the latest news on IP and read expert articles and case studies by subscribing to our email newsletter and Bulletin.

Training: We have designed a training catalogue consisting of nine different modules. If you are interested in planning a session with us, simply send us an email.

DISCLAIMER/LEGAL NOTICE