



trade secrets

# Trade Secrets: Managing Confidential Business Information

## Summary

Introduction .....	2
1. Confidential information and trade secrets .....	3
2. How are trade secrets protected in the EU? .....	5
3. TS protection management .....	7
4. Trade secrets and IP rights .....	11
5. Trade secret misappropriation .....	12
6. Conclusion - Useful Resources .....	14

\*This fact sheet was first published in March 2012 and updated in April 2021.

## Introduction

The process of research and creation leads to the development of significant information that might often not fall within the scope of the protection provided by traditional intellectual property (IP) rights such as patents or copyright. In addition, some businesses might not find it appropriate for their information to be protected through IP rights. Nevertheless, that information is valuable for business innovation and competitiveness. Therefore, it is important to keep valuable information “confidential”.

Broadly speaking, the information that is kept confidential in order to preserve competitive gains is referred to as “trade secrets”. Business and academia sometimes use other names, such as “proprietary know-how” or “proprietary technology”, to refer to trade secret information.

Some of the most well-known trade secrets include Coca-Cola’s Coke recipe, KFC chicken coating recipe, the Google algorithm, or the New York Times Bestseller List. Companies which were founded as start-ups, such as Google, owe their success largely to trade secrets that allowed them to capitalise their knowledge and attract consumers to their products.

The present fact sheet illustrates the importance of trade secrets for businesses and provides insight into trade secret protection and management, which could prove beneficial in particular to small and medium-sized enterprises (SMEs).

## 1. Confidential information and trade secrets

Confidential information is the information that must be kept secret. While any information can be confidential, not all the information generated within a company must be kept secret. The company will then decide what should be kept confidential based on the circumstances of each individual case.

In this document, we will focus on **trade secrets**.

In the widest sense, trade secrets refer to any confidential business information which provides an enterprise with an economic benefit that translates into a competitive advantage, 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.

- It is a secret in the sense that it is not known or readily accessible to a wide circle of persons;
- It has commercial value because it is secret;
- It has been subject to reasonable steps, by the person lawfully in control of the information, to keep it secret .

Trade secrets are a valuable resource to many companies whose assets may, for instance, not be patentable but have a great commercial value and therefore need to be protected. Trade secrets come in various forms, for example software algorithms, R&D information, recipes, methods, formulas, etc.

From the SME standpoint, the most highly-valued types of trade secrets are, for example:

- business methods
- market analyses
- business relationships
- pricing information
- cost information
- purchasing information
- personnel information
- office techniques
- customer or supplier lists and related data
- financial information and business planning
- R&D data
- process know-how and technology
- computer programs

- computer databases
- formulae and recipes
- ingredients
- manufacturing techniques
- manufacturing methods
- product technology
- marketing data and planning.

Trade secrets can be of the same value to businesses as patents and other forms of IP rights. They can be used as a tool for business competitiveness and research innovation management. Trade secrets also help achieve competitiveness on the market and foster innovation, often being the core of a company's operations. Therefore, any breach or disclosure of a trade secret might result in significant economic loss for the company in question.

## 2. How are trade secrets protected in the EU?

### 2.1 The Trade Secrets EU Directive

Until 2016 there were no harmonised laws related to the protection of trade secrets at the European Union (EU) level. As a solution to the uneven trade secret protection within the EU, [Directive \(EU\) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information \(trade secrets\) against their unlawful acquisition, use and disclosure](#) (the Directive) was adopted.

The Directive was key in harmonising national laws concerning trade secrets by:

- ensuring an equivalent level of protection of trade secrets throughout the Union
- introducing a uniform definition of the term „trade secret“
- providing common measures against the unlawful acquisition, use, and disclosure of trade secrets.

The Directive introduces a common set of legal principles, procedures, and protection measures with the aim of creating a pan-European regime, being an incentive for companies to invest in research and innovation in Europe with confidence. Moreover, the Directive covers the issue of infringing goods, by establishing the unlawful character of the production, offering, placing on the market, importing, exporting or storing of any goods whose design, quality, manufacturing process or marketing significantly benefits from unlawful acquisition, disclosure or use of trade secrets.

At the same time, the Directive contains several exceptions to the protection of trade secrets, e.g. to the advantage of those who reveal misconducts, wrongdoing, or illegal activity if a disclosure of a trade secret serves the public interest.

Finally, the Directive helped to make trade secret protection rules within the EU more even and interoperable, reducing unnecessary costs and barriers to cross-border innovation activities and know-how transfer.

## 2.2 Requirements for protection

Unlike patents, a trade secret does not need to be novel. Besides, its protection does not require registration, contrary to trademarks or patents. In consequence, trade secrets may be legally protected for an unlimited period of time and with no registration fees. For these reasons, the protection of valuable business information by means of trade secrets may appear to be particularly attractive for SMEs.

However, in order for such information to be classified as a trade secret, it must meet the following requirements:

- It must be kept secret;
- It must have commercial value; and
- It must have been subject to measures aimed at keeping it secret

The confidential status of information is crucial for the applicability of the trade secret protection regime. It is, therefore, particularly important for businesses to take appropriate measures to keep information secret in order to qualify for protection. Protection of trade secrets from competitors starts first within the SME itself, by setting up special procedures for handling such secrets, including technological protection measures. In addition, contractual measures can also effectively help protect secret information.

### 3. TS protection management

For trade secrets to be protected, they should first be properly identified. This means that companies should carefully audit their corporate assets to identify the trade secrets that they have. Subsequently, it should be determined who can have access to them.

In the event of a potential legal dispute, it is also useful to have a proof of ownership of the trade secret in question.

#### Did you know?

Means of obtaining date of creation includes:

- Notary seal on the document
- Public authority certification
- Witness statement
- Use date stamp mechanism provided by IP offices: envelope Soleau, i-DEPOT or WIPO Proof.

#### Helpful tools to keep information secret

- Technical protection measures
- Non-disclosure agreements
- Non-disclosure and non-compete clauses integrated in an agreement or memorandum of understanding
- Non solicitation clauses and agreements
- Document marking
- Employee activity monitoring
- Employee training

#### • Technical protection measures

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. Only the personnel needing to know 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 security personnel to trace any additions or changes back to the originator.



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.

The risk of trade secrets misappropriation comes from a variety of sources, including current and former employees, competitors and suppliers. For example, while in the telecommunications and financial sectors, former employees are of special concern, in the pharmaceutical, publishing, and financial sectors it is the competitors who usually are a company's main concern. In order to secure a company's trade secrets from both external threats and potential thefts from inside the company, the following protection measures should be implemented next to the confidentiality agreements and contractual measures mentioned below:

- clean desk policy
- employee badge policy to restrict access to specific areas and rooms
- use of passwords to protect files, folders or computers
- use of tools such as shredders, locks, etc.

#### • **Non-disclosure clauses and agreements**

As it is necessary to show that protective steps have been taken in order for a given piece of information to be considered a trade secret, businesses should consider entering into non-disclosure agreements (also called "confidentiality agreements") or including non-disclosure clauses in agreements with both employees and business partners.

NDA's help decrease the risk of disclosure of confidential information by establishing contractual obligations, whose breach may be sanctioned by financial penalties contractually agreed upon by the parties or/and involve judicial actions. Since business information may represent a dominant factor in making prospective partners decide whether to start a new business relationship, signing an NDA could prove useful before disclosure of any valuable business information at the negotiation stage .

#### • **Non-compete clauses and agreements**

Non-compete clauses and agreements are particularly useful when it comes to regulating relationships with employees or with business partners, who can usually acquire significant know-how by accessing confidential documents related to a company. It is important to safeguard that information in order to prevent the consequences that may also stem from the departure of an employee from the company or termination of a business relationship. In that case, non-compete clauses or agreements can be of help as they specify the period of time during which a former employee or a business partner is not allowed to work for a competitor or reveal certain information. Non-compete rules may be either included in the employment or partnership contracts or in a separate agreement between the parties.



• **Non-solicitation clauses and agreements**

Non-solicitation agreements are contracts in which an employee agrees not to solicit a company's clients or customers, for his or her own benefit or for the benefit of a competitor, after leaving a company. It is also possible to include such a clause in an employment contract instead of entering into a separate non-solicitation agreement. It is particularly useful to use such agreements and clauses in services where the customer pool is limited, for example, in specialised sales.

Non-solicitation agreements may be also entered into between competitors in order to explicitly agree not to solicit current employees of one or both parties.

• **Document marking**

Document marking might be crucial for employees to properly treat the documentation, avoid incurring liability, and mainly to make sure that the information is handled in a confidential manner.

Documents can be marked, among others, as:

- Confidential
- Third party confidential
- Make no copies
- Distribution limited to
- Covered by NDA

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

• **Employee training and monitoring**

Employee training should not be omitted. Employees should be informed about the company's trade secret policy and the handling of confidential information. They should know how to act outside of the company, i.e. in public spaces, with regards to trade secrets while accessing the company's e-mail and data using a public internet network, for example, and also during any commercial relationship (trade shows, exhibitions or commercial negotiations).

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 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.

**Security checklist**

- identify trade secrets in the company
- keep record of the trade secrets
- define company policy regarding trade secrets
- communicate the policy to the employees – provide training
- enter into NDAs/non solicitation agreements with employees, contractors, external partners.
- Use technical measures such as passwords, locks, badges and other policies to physically protect your trade secrets.

## 4. Trade secrets and IP rights

Trade secrets provide numerous important benefits. Firstly, trade secret protection is relatively easy to obtain as there is no requirement of registration and no examination process involved, providing an immediate right to the trade secret holder. The lack of registration requirement makes trade secrets a convenient and low-cost means of protection.

Secondly, the secret protection can cover a wide range of information. For example, an invention that is not eligible for patent protection can be claimed as a trade secret.

Trade secret protection is also potentially indefinite as long as the information is kept confidential, whereas patent or design protection are limited to a maximum of 20 and 25 years respectively. However, the degree of protection provided by trade secrets is not as high as that provided by other intellectual property laws. This is because the protection is entirely dependent on the confidential status of a trade secret. Once a trade secret is revealed to the public, it loses its secret status and therefore the protection.

In addition, IP rights provide their holders exclusive rights over their creations, which is not the case when it comes to trade secrets. Trade secret protection does not prevent competitors from copying and using the same solutions if a trade secret is obtained in a lawful manner, for example, through reverse engineering.

Trade secrets are protected solely in cases where the confidential information has been obtained by illegitimate means (e.g. through spying or theft).

Patents and trade secrets represent two of the most common methods in the technology sector to protect intellectual property. Both have advantages and disadvantages. It is useful to know the differences between them in order to choose the appropriate level of protection for your business

	PROS	CONS
Patents	<ul style="list-style-type: none"> <li>• Exclusive rights</li> <li>• Court actions</li> <li>• Base for loans</li> <li>• Involuntary infringement</li> <li>• Secure protection</li> </ul>	<ul style="list-style-type: none"> <li>• High cost</li> <li>• 20 years limited protection</li> <li>• Disclosure requirement</li> <li>• Lengthy procedures</li> <li>• Scope of protection</li> </ul>
Trade	<ul style="list-style-type: none"> <li>• No registration costs</li> <li>• Long-term protection</li> <li>• No disclosure requirement</li> <li>• Immediate effect</li> <li>• Broader scope of protection</li> </ul>	<ul style="list-style-type: none"> <li>• Not easily enforceable</li> <li>• Voluntary infringement</li> <li>• Can be reverse-engineered</li> <li>• Non-secure protection</li> <li>• Limited remedies</li> </ul>

## 5. Trade secret misappropriation

In the case of entering into NDAs or including non-compete clauses within a contract, any disclosure of confidential information can amount to a breach of confidentiality or a breach of contract. This happens when the recipient of certain business information has used that information in an unlawful way. Such a breach can lead to court litigation and monetary compensation for the trade secret holder.

The Directive lays down rules on protection against unlawful acquisition, use and disclosure of trade secrets. Namely, it is unlawful to acquire a trade secret by means of unauthorised access, appropriation, or copying of any documents, objects, materials, substances, or electronic files containing trade secrets without the consent of a trade secret holder.

In addition, the Directive allows the Member States to provide for more far-reaching protection measures against the unlawful acquisition, use, or disclosure of trade secrets than that required by the Directive.

### 5.1 How to deal with a trade secret infringement?

The Directive provides trade secret holders with a number of measures to be used against trade secret infringers. In the event of trade secret misappropriation, a trade secret holder is entitled to demand remedies, such as injunctions and corrective measures. The objective is to limit the damage caused by disclosure of a trade secret. Injunctions and corrective measures can be applied by a judge at various stages of court proceedings.

The Directive also provides a number of defenses that can be used in court by the alleged infringers (e.g. independent creation) in order to defend themselves.

A trade secret holder may also be entitled to monetary compensation (damages) based on the loss of profit or unjust enrichment.

#### **Remedies provided by the Directive**

- Cessation or prohibition of use or disclosure of a trade secret.
- Prohibition of production, offering, placing on the market, or use of infringing goods.
- Adoption of appropriate corrective measures, such as recall or destruction of the infringing goods.
- Seizure of infringing goods.

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.

## 5.2 How to deal with trade secret misappropriation accusations?

It might be the case that a company is accused of trade secret misappropriation or theft. This can, not only have a financial impact on the company, but also impact its reputation with suppliers and customers, and its goodwill with the public. For that reason, it is important to know how and when to act if such accusations take place.

If allegations of trade secret theft are made, it is crucial to undertake the appropriate steps, such as internal investigation, to try and ensure that the company's employees do not misuse the other company's information. Secure the appropriate documents and meet with the key employees to plan your response.

If the accusing party is right and trade secrets have been misappropriated, you should apply disciplinary actions within the company and seek ways to resolve the dispute in an amicable way, for example, via mediation. In addition, you should remove the unlawful trade secrets from the company or negotiate the possibility of taking up a licence from the other company in order to continue using them.

Whether or not there is truth to the accusations, you should also consider taking care of the potential harm to the company's reputation.

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

### **Trade secret defences:**

There is no trade secret misappropriation if:

- A trade secret has been an independent creation
- A trade secret was already in the public domain
- The other party did not take proper efforts to keep the information secret.

## 6. Conclusion

Companies can sometimes overlook trade secrets as assets while they might sometimes be more valuable than all of the company's patents, trademarks, and copyrights combined. The EU Trade Secrets Directive sets up a minimum standard for trade secret protection across the EU. However, in order to protect the trade secrets, companies should treat them as valuable and secret, and ensure to have a proof of having done so.

Our main goal is to support cross-border SME and research activities to manage, disseminate and valorise technologies and other IP rights and assets at an EU level. The European IP Helpdesk enables IP capacity building along the full scale of IP practices: from awareness to strategic use and successful exploitation.

## WEBSITE

The heart of our service portfolio to keep you updated



## HELPLINE

Our Helpline team answers your individual IP questions



## TRAINING

Gain IP knowledge in our free online and on-site training sessions



## EVENTS

Meet us at key networking and brokerage events and conferences



## PUBLICATIONS

Detailed IP knowledge provided through our high level publications



## AMBASSADORS

Our regional ambassadors provide IP support throughout Europe



Get in touch with us.

European IP Helpdesk  
c/o Eurice GmbH  
Heinrich-Hertz-Allee 1  
66368 St. Ingbert, Germany

Web [www.ec.europa.eu/ip-helpdesk](http://www.ec.europa.eu/ip-helpdesk)  
Email [service@iprhelphdesk.eu](mailto:service@iprhelphdesk.eu)  
Phone +34 965 90 9692 (Helpline)

## Disclaimer

The European IP Helpdesk is managed by the European Innovation Council and SMEs Executive Agency (EISMEA), with policy guidance provided by the European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG Grow).

The information provided by the European IP Helpdesk is not of a legal or advisory nature and no responsibility is accepted for the results of any actions made on its basis. Moreover, it cannot be considered as the official position of EISMEA or the European Commission. Neither EISMEA nor the European Commission nor any person acting on behalf of EISMEA or of the European Commission is responsible for the use which might be made of this information.

© European Union, 2021

Luxembourg: Publications Office of the European Union, 2021  
Print: ISBN 978-92-9460-722-5 DOI 10.2826/996749 EA-09-21-244-EN-C  
PDF: ISBN 978-92-9460-723-2 DOI 10.2826/449107 EA-09-21-244-EN-N