

## COMMENTS TO EU DIRECTIVE 2016/943 REGARDING TRADE SECRETS

1. Introduction
2. Definition of trade secrets
3. Definition of lawful and unlawful acquisition, use and disclosure
4. Non-exclusivity
5. Time limit
6. Protection during legal proceedings
7. Compensations & Sanctions
8. Conclusions & practical tips

\* \* \*

### 1. Introduction:

On June 8<sup>th</sup>, 2016, the European Parliament has published a new Directive, regarding the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. The Directive highlights that businesses, irrespective of their size, value trade secrets as much as patents and other forms of intellectual property rights.

The Directive obliges Member States to adopt the necessary legal and regulatory measures aimed to provide a better protection of commercial secrets within the EU, within a two years' term. The Directive provides some useful definitions and principles regarding the protection of undisclosed know-how and business information that can be used from now on by companies to better protect its own know-how.

Until now, such protection was mostly pursued through the legal actions established in the Unfair Competition acts, but in many occasions the result of such lawsuits was quite uncertain. After this Directive, companies that have diligently identified and protected its trade secrets should be able to reduce its unlawful disclosure, and when necessary, successfully litigate.

The present article is not a comprehensive analysis of the Directive, it just comments the points that are more interesting, in the author's opinion.

## 2. Definition of Commercial Secrets:

The advantage of the Directive in defining what are trade secrets is that it allows companies to better identify what parts of its own information and know-how can be considered as a trade secret:

Article 2 of the Directive defines as “trade secret” the information that meets all these requirements:

- a) To be secret, in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known or readily accessible to persons within the circle that normally deal with the kind of information in question.
- b) To have commercial value because of its secret character.
- c) To have been subject to reasonable measures to keep it secret, adopted by the company.

It is necessary to highlight the practical consequences of this point “c” of article 2: Companies should have adopted the necessary measures to keep the know-how secret, which in practice implies the need of elaborating a protocol establishing the legal, human and technical measures to protect the company’s know-how from unauthorized –even involuntary- disclosure by directors, managers, employees, purveyors, clients and franchisees (and the same range of persons within the franchisees’ businesses: owners, managers, employees, etc.).

The Directive mentions that commercial secrets extend to a diverse range of information, including not only technological knowledge, but commercial data such as information on customers and suppliers, business plans and market research and strategies.

The Directive also says that the definition of commercial secrets should include:

- Know-how
- Business information
- Technological information,

Provided that there is both (i) a legitimate interest in keeping it confidential and (ii) a legitimate expectation that the confidentiality will be preserved.

Besides, such information should have commercial value, real or potential. It is considered that the information has commercial value when its unlawful disclosure could damage the interests of its legal owner.

Non relevant information and the information that it is easily accessible within the circles where it is usually used is excluded from the definition of commercial secrets.

Employees:

The information and capabilities acquired by employees during the normal course of their professional career is excluded from the definition of commercial secrets. In order to prevent the lawful, but potentially damaging, use of such information and capabilities, employees could be subject to non-competition commitments, through the correspondent clauses included in their labor agreements. Such clauses are subject to some time limits; in Spain, for example, this limit is two years after the termination of the labor agreement, and the employee should receive a compensation for such limitation. Because of this obligation to compensate, post-agreement non-compete clauses should be included only in the labor agreement of those employees whose knowledge and contacts are relevant, otherwise the company would be paying non-compete compensations to employees whose incorporation to a competitive company does not cause any damage.

### 3. Definition of lawful and unlawful acquisition, use and disclosure:

Article 3 of the Directive defines as lawful acquisition of trade secrets when they are obtained by any of the following means:

- a) Independent discovery or creation
- b) Observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information, who is free from any legally valid duty to limit the acquisition of the trade secret.
- c) Exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national law and practices (this right to information does not allow however to the disclosure or commercial exploitation of such trade secrets).
- d) Any other practice which, under the circumstances, is in conformity with honest commercial practices.

And article 4 defines when the acquisition of a trade secret without the consent of its holder shall be considered unlawful:

- a) Whenever carried out by unauthorized access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deducted.
- b) Any other conduct which, under the circumstances, is considered contrary to honest commercial practices.
- c) Whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions:
  - i) Having acquired the trade secret unlawfully

- ii) Being in breach of a confidentiality agreement
- iii) Being in breach of a contractual or any other duty to limit the use of the trade secret.
- d) Whenever a person, at the time of acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

#### 4. Non-exclusivity:

The Directive mentions that its provisions should not create any exclusive right to know-how or information protected as trade secrets. Thus, the independent discovery of the same know-how or information should remain possible. Reverse engineering of a lawfully acquired product should be considered lawful, except when otherwise contractually agreed. The freedom to enter into such contractual arrangements can, however, be limited by the law (regarding this point it will be necessary to pay attention to how each EU member state adapts its domestic laws).

#### 5. Time limit:

The Directive requests member states to establish a time limit for the start of legal claims, which should not be longer than 6 years, and to establish, in a clear and unambiguous manner, from when that period is to begin to run and under what circumstances that period is to be interrupted or suspended.

#### 6. Protection during legal proceedings:

The Directive notes that many times, the risk of losing the confidentiality of a trade secret deters its legitimate holder from instituting legal proceedings when there has been an unlawful disclosure. Therefore, the Directive requests member states to ensure that the parties, their lawyers, court officials, witnesses, experts and any other person participating in legal proceedings are not allowed to use or disclose the trade secrets that have been identified as confidential. These measures shall at least include the possibility of

- a) Restricting access to any document containing trade secrets
- b) Restricting access to hearings to a limited number of persons
- c) Making available non-confidential versions of any judicial decisions

## 7. Compensations & Sanctions:

The holder of a trade secret should be entitled to compensation of damages appropriate to the actual prejudice suffered, which could include:

- Lost profits which the injured party has suffered
- Unfair profits made by the infringer
- Moral prejudice caused to the trade secret holder
- Alternatively, the judicial authorities may set the damages as a lump sum on the basis of elements such as, at minimum, the amount of royalties or fees which would have been due had the infringer requested authorization to use the trade secret in question.

Member States may limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer where they act without intent. In the opposite sense, this paragraph implies that employees could be considered liable for the disclosure (even without intent) of a trade secret, and therefore, it should be possible to include in their labor agreements the necessary clauses to remind them the confidentiality obligations they have towards the company's secrets, and the penalties or compensations they may be obliged to pay in case of breach of such obligations, especially in case of breach of the company's protocol. Such penalties may be different in case of involuntary disclosure or voluntary but unlawful use or acquisition.

The competent judicial authorities may impose sanctions on any person who fails or refuses to comply with any measure adopted pursuant to articles 9 (confidentiality during legal proceedings), 10 (provisional and precautionary measures) and 12 (injunctions and corrective measures). The sanctions should be effective, proportionate and dissuasive.

## 8. Conclusions & practical tips:

The Directive is not directly applicable to companies, but to the EU Member States, requesting them to approve the necessary measures to provide a safer legal frame for the protection of trade secrets, within a two years term.

Notwithstanding the above, the principles and definitions of the Directive could be used from now on by EU companies in order to protect better its know-how, especially in view of the fact that having taken the due diligence will be a requirement for obtaining favorable Court judgments.

The due diligence action plan that any company should take could consist in the following steps:

- i) Create a commission or working team, formed by the at least one representative of the HHRR, the IT and the Legal departments (in-house or

external). Depending on the sector of activity, other departments (i.e. R&D) should be involved.

- ii) Make an inventory of the existing commercial secrets and identify the departments or teams that are more likely to develop commercial secrets in the future.
- iii) Evaluate the existing protection measures. Specially review the company's policies regarding the use of information and communication technologies: PC's, laptops, smartphones, pen-drives, e-mail, VPN, data bases, etc.
- iv) Evaluate what clauses are included in the labor agreements, and if necessary re-draft them. The clauses should be as complete as possible for key employees, but other employees should have easier clauses. Review the procedures used for dismissals and make sure that dismissed employees have no remote access to confidential information. Review and if necessary amend the company's policy regarding monitoring the employees' use of the company's devices (smart phones, e-mail, etc.)
- v) Review what information is disclosed to other parties: Board Members, shareholders, purveyors, clients, franchisees or distributors, etc. Draft the necessary confidentiality clauses, including recommendations to avoid involuntary or careless disclosure of information.
- vi) Create a protocol including the conclusions of the above points. Make sure the protocol is widely known and applied within the company.
- vii) For franchising companies, adapt, and if necessary simplify, the above protocol and apply to the franchisees. Monitor the implementation of the protocol by the franchisees.

Mercedes Clavell  
Lawyer  
ARCO ABOGADOS – SPAIN  
mercedesclavell@arcoabogados.es