

Protection of trade secrets in Ukraine

Introduction

1. Trade secrets in Ukraine

2. Protection of trade secrets

3. Organising trade secret protection in a company

B

Protection of commercial information in Ukraine has certain peculiarities, primarily due to the specifics of its legal regulation.

At a first glance, information security in a company is the prerogative of its security service. However, in Ukraine, measures aimed at protecting trade secrets must not only be physically effective, but also have clear regulation within the company and comply with Ukrainian law.

1. Trade secrets in Ukraine

Ukrainian law defines a trade secret as information that is secret, i.e., unknown and difficult to access. At the same time, such information:

- is not available to those persons who could potentially use it;
- has commercial value primarily because it is not known to third parties;
- is protected by the company;
- if used by third parties without the company's permission or control, may cause damage to the company.

In Ukraine, trade secrets may include information of a technical, organisational, commercial, production or other nature.

In particular, this includes information about the company's financial and administrative development plans, concluded (planned) contracts, customers, counterparties, new technical projects and methods of labour organisation and production, the size of the trade margin, discounts

on the purchase of products, the volume of purchases and deliveries of products, confidential information about an individual (personal data, marital status, health status, etc.).

Trade secrets may be contained in agreements, contracts, reports, analytical materials, extracts from accounting records, specifications and other documents reflecting the company's activities. Ukrainian law does not establish a specific list of information that may be deemed a trade secret.

The composition and scope of information constituting a trade secret is determined by each company independently. However, the Government of Ukraine has established a list of data that cannot be classified as a trade secret.

The list includes:

- constituent documents, documents authorising the company to engage in entrepreneurial or business activities and its individual types;
- information on all established forms of state reporting;
- data required to verify the calculation and payment of taxes and other mandatory payments;
- information on the number and composition of employees, their salaries in general and by profession and position, as well as the availability of vacant jobs;
- documents on payment of taxes and mandatory payments;
- information on environmental pollution, failure to comply with safe working conditions, sale of products harmful to health, and other violations of Ukrainian legislation and the amount of damage caused;
- documents on solvency;
- information on the participation of company officials in cooperatives, small enterprises, unions, associations, and other organisations engaged in entrepreneurial activities;
- information that is subject to disclosure under effective legislation.

This list is rather archaic. It was established long before the adoption of the Civil Code of Ukraine, which stipulates that the list of information that does not constitute a trade secret may be established exclusively by law. Therefore, it may seem that today any information that meets the above criteria can be classified as a trade secret.

However, there is no court practice that would unambiguously address this matter, and the list itself is widely used primarily by state regulatory authorities. Therefore, a more balanced position would be to take into account the requirements of the Cabinet of Ministers of Ukraine when compiling a list of information containing trade secrets.

In addition to the aforementioned list, it should also be borne in mind that Ukrainian law establishes a general list of information access to which cannot be restricted. This includes, in particular, the following information:

- on the environmental situation;
- on the quality of food products;
- on accidents, disasters and emergencies, public health, etc.

It is worth keeping these restrictions in mind when compiling a list of information that constitutes a company's trade secret, as trade secrets are classified as restricted information.

In Ukraine, a trade secret is an object of intellectual property. Accordingly, the company owns intellectual property rights to trade secrets, in particular:

- the right to use trade secrets;
- the exclusive right to authorise the use of trade secrets;
- the exclusive right to prevent unlawful disclosure, collection or use of trade secrets;
- other intellectual property rights established by Ukrainian legislation.

2. Protection of trade secrets in Ukraine

Ukrainian labour law does not contain the concept of a trade secret. However, every employer is obliged to create conditions to prevent employees from disclosing trade secrets. This approach is also supported by court practice.

The issue of trade secret protection in relations with contractors is also regulated rather poorly. Filing a lawsuit for recovery of contractual penalties for disclosure of trade secrets or damages in the form of lost profits and an appeal to the Antimonopoly Committee of Ukraine are virtually the only instruments that can potentially help protect trade secrets in contractual relations. At the same time, there is no sufficient court practice on this issue in Ukraine.

The law provides for liability for disclosure of trade secrets, including:

civil liability in the form of damages

The court practice in Ukraine shows that the application of this type of liability is not effective enough. This is because of the difficulty of

proving both the amount of damages and the link between the damages and the actions of a person who disclosed a trade secret. In claims for compensation for lost profits, it is also necessary to prove the possibility of obtaining the lost profits.

disciplinary liability

Ukrainian labour law does not regulate liability for disclosure of trade secrets. However, disclosure of trade secrets may be qualified as a breach of labour discipline and may result in dismissal or reprimand. For this purpose, as the court practice shows, a breach of labour discipline should only relate to those duties that are part of the employee's job function or arise from the internal labour regulations.

administrative liability

Ukrainian administrative legislation provides for a fine of up to UAH 24,000 (EUR 600) for disclosing trade secrets and other confidential information with the intent to damage the business reputation or assets of another entrepreneur.

criminal liability

The criminal law of Ukraine provides for a fine of up to UAH 4,000,000 (EUR 100,000) with prohibition to hold certain positions or engage in certain activities for up to 3 years. Such liability is imposed for intentional disclosure of commercial, banking or professional secrets in the capital markets and organised commodity markets without the owner's consent by a person who knows the secret in connection with his or her professional or official activities, if such disclosure is made for profit or other personal reasons and has caused significant damage to the company. In addition to these types of liability, a company in Ukraine may seek protection of its infringed trade secret rights from the Antimonopoly Committee of Ukraine under the legislation on protection against unfair competition.

3. Organising trade secret protection in a company

The system for protecting a company's trade secrets in Ukraine should include a coherent and manageable procedure that takes into account the following:

- any employee of the company should be strictly prohibited from disclosing information that is regarded as a trade secret; establishing a single trade secret regime for certain information;
- procedures for the protection of trade secrets should be standardised and should include: familiarising all employees with such procedures;
- creation and implementation of standard procedures for responding to requests from third parties (courts, lawyers, government agencies, police, etc.) for disclosure of information containing trade secrets;

- timely amendments to the list of information that constitutes a trade secret.

the content of contracts and other documents concluded or used by the company in its relations with third parties should be controlled for provisions on the preservation of trade secrets and the establishment of liability for their disclosure;

hiring and dismissal of employees should be accompanied by non-disclosure agreements;

the company must always have evidence that employees have been familiarised with the list of information that constitutes a trade secret.

Therefore, the minimum measures aimed at building and implementing a trade secret protection system in a company should include:

- creation and approval of a list of information that constitutes a trade secret by the company's head;
- obligations to maintain trade secrets in employment contracts and job descriptions. It is important that any breach of such obligations be treated as a breach of labour discipline;
- creation and implementation of policies and standard procedures related to the use, preservation, and disclosure of trade secrets and employees' liability for unlawful dissemination of information constituting a company's trade secrets;
- provisions on trade secret protection in contracts with counterparties;
- signing separate non-disclosure agreements with employees;
- defining procedures for controlling the use of personal computers, internal networks, the Internet, removable storage devices, and printers by employees.

The basic procedure for building a trade secret protection system in Ukraine is to determine the list of information that is considered a trade secret in the given company.

The information specified in such a list should:

- contain data obtained and created (including as a result of information processing by technical means) by the company;
- be useful and used by employees for their work in the company and be necessary for the normal functioning of the company;
- be restricted for use;
- be primarily related to the production, management, financial or other economic activities of the company;
- potentially harm the interests of the company as a result of its disclosure;
- meet the criteria established by Ukrainian legislation.

In practice, the list should take into account the balance of potential losses arising from the disclosure of trade secrets and the costs for their

protection.

In order to determine the potential losses and negative consequences of disclosure of trade secrets, the company's actual circumstances should be assessed, e.g:

- the degree of importance of non-disclosure of information about the profit-making process in the fight against a competitor;
- the possibility of winning in time when creating competitive products or services;
- whether the company has a monopoly on a technology it owns;
- the likelihood that the information will be used by a competitor if it is disseminated.

The quantitative and monetary indicators of potential losses should be determined by the level of efficiency reduction in the production or financial side of the company's activities, while the qualitative indicators should be determined by the degree of possibility of lost profits.

Potential negative consequences that should be considered include the following:

- severance of relations or reduced level of cooperation with business partners and customers;
- failure to fulfil contractual obligations;
- difficulties in the supply, production and sale of products or services;
- economic sanctions against the company.

Of course, the establishment of a legal regime for the protection of trade secrets in a company is meaningless if it is not accompanied by its practical and technical implementation. However, a clear regulation of relevant procedures will not only streamline such measures and make them more effective, but also create conditions for protecting the company in Ukraine in the event of leakage of information constituting a trade secret, hostile actions of competitors or unlawful actions of regulatory authorities.