Published on *The National Law Review* https://natlawreview.com

New German Trade Secrets Law: Next Steps for Businesses

Article By:

Dr. Henrik Holzapfel

Dr. Martin Königs

Germany recently introduced a new act that will substantially change the way trade secrets are protected. As the term is used in Germany, “trade secrets” include both technical know-how (such as construction drawings, manufacturing methods, ingredients and recipes) and business information (such as customer data, purchase prices and market studies). The first draft of the new act was presented on April 19, 2018, and some of the changes are already relevant. Enterprises doing business in Germany should be aware of the new opportunities, risks and requirements under the act:

- Only information that is subject to actual and reasonable measures to maintain secrecy will be protected as a trade secret. As a result, enterprises may have to adopt additional contractual, organizational and technical measures to protect their trade secrets. In order to be in a position to enforce trade-secret-derived claims against third parties, enterprises should immediately start documenting the protection measures they adopt.

- Reverse engineering is permitted, except when otherwise contractually agreed. Enterprises therefore may want to include clauses against reverse engineering in agreements with third parties such as suppliers, customers and R&D partners. However, reverse engineering will still be possible for competitors and other third parties.

- Under the new law, an enterprise may be liable for infringement of trade secrets even if its management has not acted culpably. This change facilitates enforcement against competitors but at the same time creates risk in terms of defending against third-party claims.

- In addition to claims for injunctive relief, damages and information, infringers may be liable for recall and destruction of products that were manufactured and marketed as a consequence of infringement of a trade secret.

The basis of the new act is EU Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets). This Directive had to be implemented into national laws by June 9, 2018. Where the Directive has not yet been implemented, such as in Germany, individuals may to a certain extent rely on the Directive itself, arguing that the existing national law must be construed in a way that brings it in line with the Directive.

Therefore, enterprises doing business in Germany should take the following steps:

- Establish a process for identifying and categorizing proprietary information and the people who have access to such information, and evaluate the protection status. This process should be reviewed and conducted on a regular basis, because new information may be generated continuously.

- Make a strategic decision about the extent to which secrecy is sufficient to protect proprietary information, and whether intellectual property rights, such as patents, should be obtained. Secrecy gives no protection against independent developments by competitors, and maintaining secrecy of technical information may become increasingly difficult as powerful technical means of reverse engineering continue to emerge. Patents also can provide effective protection against a competitor's subsequent independent developments. Patents are easier to license out and may be easier to use for advertisement purposes. At the same time, patents have a limited lifetime, make proprietary information available even in regions where no protection is sought, and are associated with costs such as annual renewal fees.

- Define clear responsibilities and access rights for proprietary information. The more important the secret information is for the company's business, the more restrictive its access rights should be. This applies both to internal access and to provision of information to external parties, such as customers. Access to important and proprietary information should be granted on a need-to-know basis only. It is also helpful to establish a safety culture through regular training and clear rules for dealing with private and business IT devices such as storage media, and regarding what data that may (or may not) be taken on business trips abroad.

- Make use of available contractual means to protect secrecy, such as confidentiality clauses in employee contracts and post-contractual non-compete clauses. The latter should only be considered in contracts with key employees, because these clauses must be drafted in a case-specific manner, and a post-contractual restraint will incur costs for the employer. Trade secrets also must be protected (especially against reverse engineering) in contracts with third parties such as customers, suppliers, licensees or R&D partner via non-disclosure agreements (NDAs). NDAs often include contractual penalties.

- Establish IT measures to protect secret information. Such measures include firewalls, encryption, monitoring access to information, and rules on the use of private storage media.

National Law Review, Volume VIII, Number 208