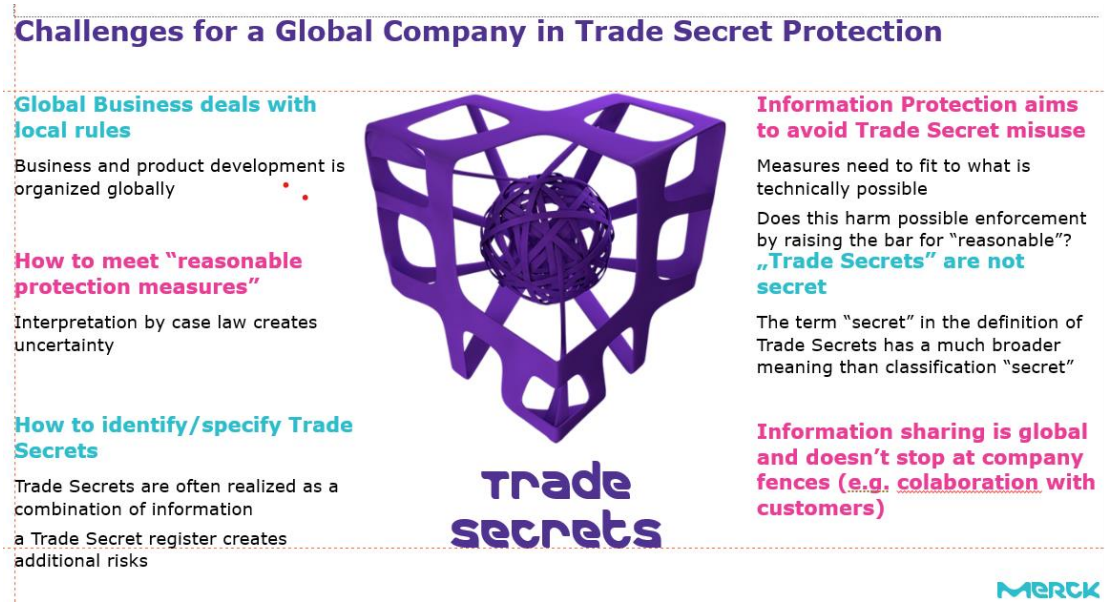
Business Insights in Trade Secret Management

The Secret Protection across businesses and countries

Dr. Stefan Horstmann
Vice President PS Core, Patents and Scientific Services
Merck KGaA, Darmstadt, Germany

Introduction

Merck KGaA, Darmstadt, Germany, and its affiliated companies (the “Merck Group”) operate as a global leader in pharmaceuticals, life sciences, and electronics. The company was founded in 1668 and established industrial scale production as well as global market activities already in the 19th century. Today, with over 63,000 employees and operations in approximately 70 countries, Merck is a global leader in the pharmaceutical, life science and special chemical industries. In 2023, Merck reported revenues of €21 billion, reflecting its significant presence and impact in the global market. The company's product portfolio includes pharmaceuticals, biopharmaceuticals, specialty chemicals, and high-tech materials, all of which rely heavily on cutting-edge research and development. This is reflected by a spent of 2.3 billion Euro for R&D activities in 2023. The business portfolio of the Merck Group is actively managed and characterized by major acquisitions during the last decade, such as Sigma-Aldrich, AZ Electronic Materials, Versum Materials and most recently the startup Mirus Bio, as well as divestitures, such as the recently announced planned sale of the Surface Solutions business. An essential skill to do such deals is the ability to keep these business secrets sealed during the preparation and negotiation phase. As a publicly listed company insider rules apply to major financial KPI and business strategic information – another huge trade secret asset of the company.



Sector Specificities

The business sector “Healthcare” in Merck operates the pharmaceutical business, including new medications to treat conditions such as cancer or multiple sclerosis (MS), but also innovative technologies that make life easier for patients. As the global market leader in fertility treatments, this business sector has helped many women and couples to achieve their dream of having a baby. All these Healthcare businesses rely on strong R&D providing a pipeline of innovation, supported by business development activities – mainly focused on in and out licensing - to manage the product pipeline. While transparency about product properties and safety for the patients are the key success factor for this business, trade secrets matter in early stages of the research, as well as biopharmaceutical production processes.

The business sector “Life Science” focusses on tools, services and digital platforms to empower researchers from a wide range of fields — from small labs to massive operations — to work more effectively. This business includes a unit called Science and Lab Solutions, comprising an online platform selling chemical and biological products, as well as a unit called Life Science Services with services around drug manufacturing, testing and analytics. In the business called Process Solutions products for the pharmaceutical industry – traditional formulations as well as novel modalities – are the core offering. In partnering with pharmaceutical customers during their R&D activities, protection of our customers trade secrets is a key value and a necessary part of the offer.

The business sector “Electronics” defines themselves as the company behind the companies, advancing digital living. The focus is on the electronics market with materials and solutions, mainly for the display and the semiconductor industry. While there is a product catalogue with a broad offering of specialty gases and precursors, as well as equipment for handling of these chemicals, many products are developed or optimized in close collaboration with a partner – typically a customer such as a display panel or semiconductor device manufacturer. Again, trade secret protection of our know how in these collaborations as well as the customers development targets is key to enable the innovation driven market strategy of this business sector.

Overall, trade secrets at Merck encompass a wide range of confidential information, including business methods, pricing information, R&D data, and manufacturing methods. Key assets are R&D databases connecting chemistry and biology with the pharmaceutical or industrial application (e.g. “structure-property-correlations”), as well as the ability to firewall the confidential information of our partners within our organization. The competitive nature of Merck's sectors necessitates robust Trade Secret protection to maintain a competitive edge and secure sensitive information.

Internal Policies and Protection Measures

The trade secret policy

To protect these valuable trade secret assets of the company many functions need to work hand in hand. The overall framework of trade secret protection is defined in a global trade secret policy. This policy is in force for the entire global organization and defines trade secret protection as an integral task of all managers for their area of responsibility.

A globally available training for all these managers is a core element of the unified approach to trade secret protection within the company.

Many specific protection measures are defined and implemented by functions with global responsibility and oversight. This includes for example, standards for site security and cybersecurity, confidentiality terms in employment agreements and guidance for onboarding and exit interviews of employees, as well as a publication release service and guidelines for protection of trade secrets in relationships to third parties, e.g. through confidentiality and collaboration agreements.

Awareness is a permanent challenge.

A permanent challenge in a big global organization is to keep up with the ongoing change of the organization – literally every day somebody moves to a new role and responsibility - and often entire businesses are restructured with an impact on the ownership of important trade secrets. Driven by the variety of businesses and complexity of organizations, a decision was taken, not to centralize trade secret management as such, e.g. not under the responsibility of a central organization. In other words, while the coordination of protection efforts is done on a global and central level, the responsibility for the trade secret is with each team and specifically each manager for the individual area of responsibility.

Looking into the layers of trade secret protection, the core is a culture to value confidential information, and especially trade secrets, as an asset of the company. Closely connected to that is awareness for the need to protect trade secrets among all employees. This is inter alia addressed by country or business specific communication campaigns to increase the awareness in the organization. Also, the internal compliance network addresses this and even encourages employees to speak up, when they notice trade secret misappropriation – as appropriate, directly or anonymously through speak-up lines. trade secret trainings for all employees, as well as addressing the topic in the onboarding process of new employees and more specifically in the exit process, are other pieces helping to create awareness. In critical areas the exit process includes signature of a declaration, documenting that the leaving employee is aware of the ongoing obligation to keep confidential information of the company confidential.

information classification and trade secret identification

A next layer is a set of information protection measures, such as access control to sites, buildings, rooms as well as computer systems and data sources. While classification of information as such is a recommendation for our teams, the tools used to store and process such information are strictly classified, and the protection measures are adjusted to the classification level of such tools and databases. For example, a database created and used in research comprising physical and application properties of chemical compounds for one business is definitely a major trade secret asset of that organization. On the other hand, the information stored in that database is updated with every new data point created. More than 6000 employees in R&D create many data points every day, which comprise a combination

of publicly available information, internal information and confidential information. Even the classification of this information might change from confidential to public, e.g. if a patent application describing a new compound and its properties is published. But the entire database stays a major trade secret asset and even growth in value with every new data point.

For inventions, there is a mandatory evaluation done, whether to apply for patent protection or whether to seal those as tradesecrets. When the inventors provide an invention disclosure, a central process that is part of the Merck Group wide patent portfolio management process is initiated. It involves at least a senior patent counsel and the responsible R&D manager, and in most cases, also a marketing manager of the relevant business. If the decision is to seek patent protection, the patent counsel has the responsibility to file a patent application. In case the decision is to seal the invention, this process is also initiated in the central patent department of the Merck Group. The invention disclosure file is turned into a trade secret file and sealed. It is important to note that the Merck Inventor Award Standard recognizes and awards invention disclosures that are sealed as trade secrets, like those that result in patents.

trade secret insiders

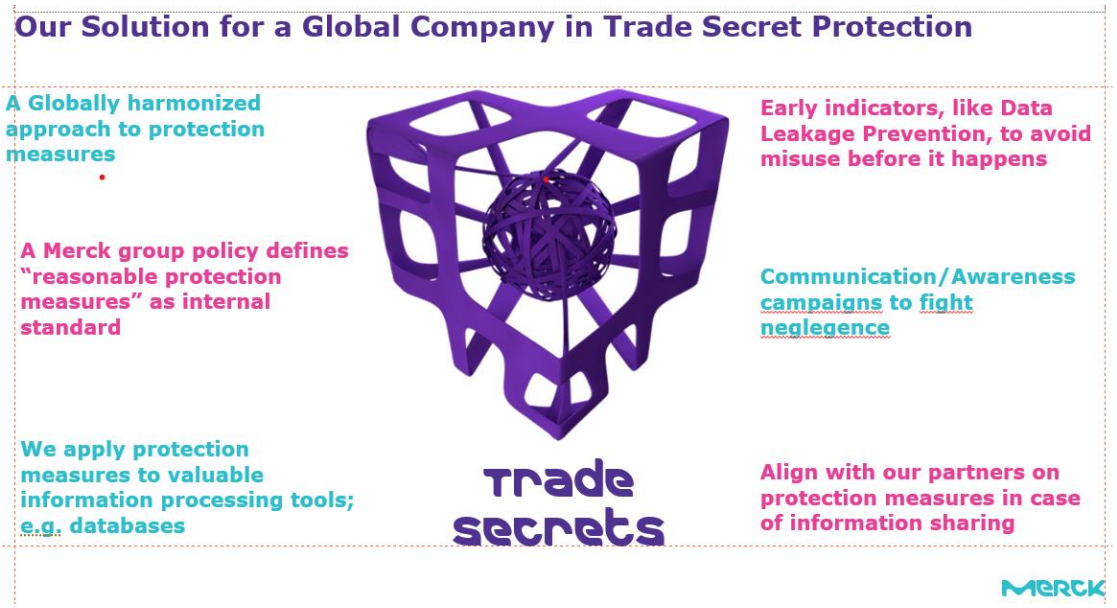
A special trade secret insider status for employees exposed to high value trade secrets in their everyday business seems desirable from the view of trade secret protection. Systematic implementation of such a special measure for all those employeestrade secret on a global scale suffers from the huge differences in labor law between the different countries and even between the different states in, for example, the United States. For example, the obligation imposed on employees to stay away from direct competition after the end of an employment can be valid and enforceable in one state, while it is void in the neighborhood. Therefore, such strict anti-compete rules typically apply to employees only in specific project situations or are applied in a threatening exit scenario.

data leakage prevention

In the cybersecurity area, protection against external attacks and attempts to steal data dominates. One aim is to detect copying of data before information leaves the company. Systematic data leakage prevention software installations are supposed to fulfill this purpose. Nevertheless, the threshold of such systems needs to be adjusted in a manner that is balancing on the one hand the risk that data is removed and on the other hand the need to follow up also on false alerts.

the need-to-know principle

Information sharing on a need-to-know basis is another principle of trade secret protection. This works well in areas with stable organizations and well-defined roles, like finance reporting or in operations, where only few people in a factory need access to information about the entire production process. The need-to-know principle can also be systematically managed in project work, such as specific R&D or business development projects. But there is an imminent conflict between fostering innovation and out of the box thinking – Curiosity is a value as such in the Merck Group - and the strict implementation of the need-to-know principle.



Trade Secrets and external relationships

Due to the innovative nature of the businesses of the Merck Group, there is a permanent need to share trade secret information with partners. This includes the need to share own trade secrets, for example R&D results, with potential customers during the product development phase. In addition, Merck needs to protect trade secrets of partners. Typical examples are in the Life Science business, where development services and analytical services are provided to partners doing pharmaceutical research and development. Similar situations happen in the Electronics business area. New display modes or advanced semiconductor production technologies are developed and optimized in close collaboration between the producers of these devices, material suppliers and sometimes also equipment manufacturers. For those businesses relying on exchange of valuable confidential information as part of the business model, the ability to trustworthy handle and protect these trade secrets of third parties is very important for the reputation of the company and the reliability as a partner.

Trade secret protection in these collaboration situations starts with contract terms addressing the expectations of both parties regarding the protection standards to be applied and lives from their ability to implement the agreed standards in the work environment. In extreme cases, already the existence of the agreement and the collaboration as such is regarded a trade secret and need to be sealed within a small team in the company. These projects typically require firewalling the received information. The data must be excluded from the "normal" information sharing between databases through automated data exchange and often require the ability to delete data again from the systems, once a collaboration ends. Workbenches with permanent video monitoring – available online to the partner - are another extreme example of implemented protection measures, in some situations. Specific measures can, for example, involve a need to identify all employees getting access to the information.

A comparably new challenge is the handling of data from partners in big data analysis. Often it is a desire of both parties that also the data provided by the partner can be used to train artificial intelligence or to detect patterns in big data sets, as long as it can be made sure that the information comprised in the data will not become available to the other party. In exceptional cases, the solution can be to have a third party analyze the datasets and share the findings with both partners. In the meantime, this even evolved into a business model

within the Merck Group. There are already two joint ventures established by the Merck with external partners. These companies are firewalled from the Merck data world and have the business model to analyze data from different partners in combined datasets.

Another aspect related to the valuation of third-party trade secrets is the onboarding process of new, but already experienced employees- especially in R&D. New joiners learn that Merck wants to stay clean form information belonging to other companies such as former employers, being it trade secrets or just owned data and information. Challenging inventions made by new joiners during the first few months with the company is a good practice in that regard.

Since also other companies work in a similar environment, the classical due diligence in an in-licensing project comprises a challenge of the ownership of registered Intellectual Property. It would be desirable to extend this to the trade secrets and all R&D results, but by the nature of these secrets, the necessary details are usually not available.

Enforcement of Trade Secrets

The aim of trade secret protection is to avoid the loss of valuable confidential information. Therefore, legal enforcement of trade secrets is only the plan B, if the intended protection failed.

The typical situation calling for trade secret enforcement is: an employee has left the company and either established an own business directly competing with the business the employee was involved in before or works in a prominent role with a competing company. In such cases, there are all kinds of rumors about misappropriation of trade secrets exist within the business organization. The challenge for the investigator team in preparing the case is then to identify the hard facts – what information was taken, does this information qualify as trade secret and is this information used by the former employee in the new business context. Many alleged trade secret misappropriation cases fail in this internal investigation phase. Depending on the jurisdiction, hurdles are the standards of evidence needed to establish a case with a good chance to be successful, and the risk that information that is supposed to stay confidential becomes publicly available through the court procedure.

On the other hand, it can often be shown that the leaving or former employee has copied or taken confidential information. In these cases, violation of the confidentiality obligation in the employment agreement is a good basis for enforcement. This works even better in early stages, before damage to the business happens, or there is no, or no big damage involved. Citing such examples during trade secret awareness campaigns and trainings in an anonymous but still exemplary manner increases the impact of such communications significantly. Similarly, published successful enforcement cases against competing companies can be used case studies for internal communication purposes.

Conclusion

Trade secret protection in a multinational science and technology company with multiple businesses, such as the Merck group can hardly be organized by a static central organization but requires many group or enabling functions to provide reasonable protection measures, as required by the legal definition. The protection itself is founded on the awareness for the value of trade secrets and based on protection measures applied in many decentral teams owning the valuable information.

By fostering a culture of awareness and implementing stringent internal and external policies, Merck aims to protect its and its partners' valuable trade secrets, maintaining its competitive edge and driving innovation across its sectors.