Know-how protection 4.0

Strategies for safeguarding your business model

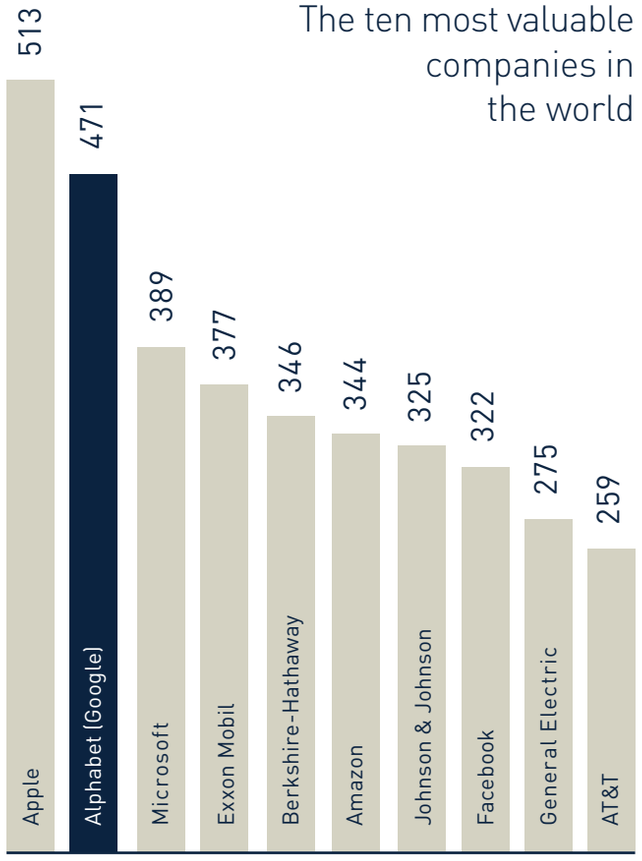
Introduction

Google was established on 4 September 1998. That was 18 years ago. The internet group has come of age and has shown what a company can achieve in the digital era, even in its early years: in 2015, it had turnover of 74.5 billion dollars and profits of 23.4 billion dollars. In February 2016, Google even briefly took Apple's place as the most valuable company in the world. And here is what lies behind that success: three million search queries are sent to Google worldwide every minute. That creates a flood of data, from which Google can make money.

Of the ten most valuable companies in the world, five are technology companies that generate their added value through innovation, algorithms and data – all of them from the USA. However, the monetisation of data and the development of digital services are areas that also offer huge opportunities for German companies. The German automotive industry's worldwide sales are in the tens of millions. The German engineering sector is delivering equipment worth 260 billion euros. Logistics operators in Germany are handling a transport volume totalling around 4.5 billion tonnes. All this business creates data – but what are German companies doing with this wealth of data?

The foundations of success in the digital transformation are innovations and know-how. These assets need not only to be used, but also to be protected. In this white paper, we discuss the requirements that know-how protection needs to meet in the course of the digitalisation of German industry.

The ten most valuable companies in the world



Market capitalisation in $ bn (as on 30.06.2016)
Source: *EY*

Background

Digitalisation is changing companies and markets

*A wave of digital innovations under the name **"Industry 4.0"** is currently heading towards manufacturing companies. These innovations are making huge changes to production processes and the stages of the value chain. The consequences are a higher level of efficiency and completely new possibilities in the development and delivery of products.*

Machine-to-machine communication

In the digital factory, machines communicate independently with each other. New potential for automation is being exploited as a result.

Big data

Machines are equipped with more and more sensors and produce more and more data, for which there are increasingly better analysis instruments. This wealth of data can be used to extract more insights and to derive new digital business models.

Human-machine interfaces

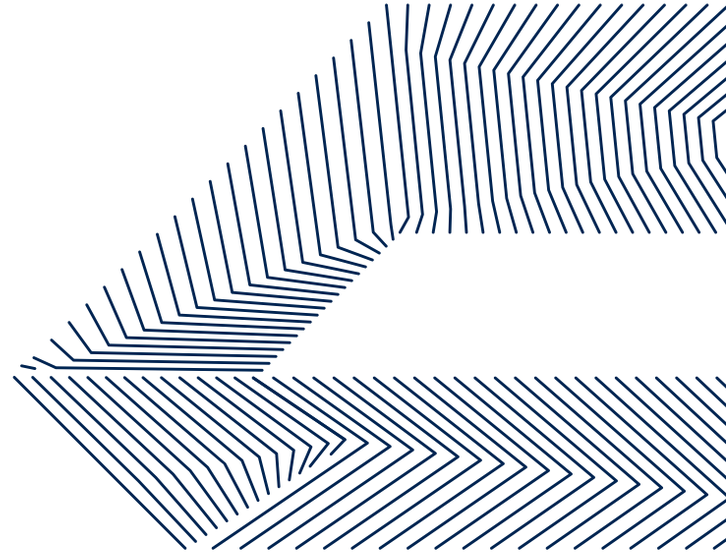
In Industry 4.0, machines actively speak to the relevant skilled workers in the factories. For example, specialist workers have mobile devices on which they can find information about current or impending faults. This prevents processes coming to a standstill or shortens the duration of such stoppages.

3D printers

Decentralised manufacturing close to customers is becoming possible with the help of 3D printers. In this way, production is returning to urban spaces. Even small production volumes can be handled cost-effectively.

Lot size one

The goal of Industry 4.0 is mass production with a lot size of one. Increasingly flexible and better-networked production systems are making greater product diversity possible.



Protecting digital business models

Data and algorithms are central trade secrets

Know-how that is worth protecting is found in every company in a very wide variety of forms. As a rule, trade secrets exist mainly in the technological and commercial fields.

Technological know-how
- Software
- Algorithms
- Construction drawings and design sketches
- Materials and formulations
- Research results
- Unpublished prototypes
- Inventions that are unpatentable or have not yet been patented
- Proposals for improvement
- Production processes

Commercial know-how
- Customer/user data
- Marketing and sales concepts
- Business plans
- Business practices and strategies
- Internal cost structures
- Price information
- Supplier data
- Ideas for product names

Data and algorithms, which are used for collection, analysis and networking, are absolutely central trade secrets in digital business models. Accordingly, the access to know-how and the scope of that access need to be managed professionally.

Especially in Industry 4.0 ecosystems, there is considerable networking of know-how-intensive units. This creates new trade secrets, but, at the same time, the risks of the loss of existing know-how are multiplied. As a result, in addition to fair models for sharing future financial results, the handling of relevant know-how and the protection of trade secrets within the network are issues that have to be resolved. This poses the question of how know-how can be protected even in highly networked innovation landscapes.

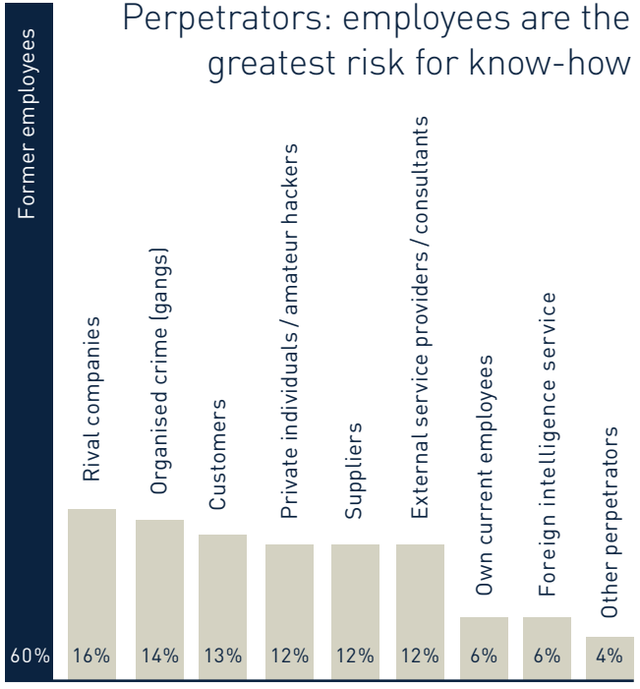
Identifying potential hazards

Employees, cooperation partners and competitors can have an interest in trade secrets

Theft of secrets is not uncommon, as surveys demonstrate. According to a study conducted in 2016 by the German Federal Association for Information Technology, Telecommunications and New Media (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. – Bitkom), 69% of companies were affected by industrial espionage, sabotage or data theft over a two-year period. A further 20% indicated that their company had probably been affected. The losses resulting from this have been estimated at 44.7 billion euros over the past two years.

Statistically, more company secrets find their way to inquisitive competitors through employees than as a result of hacking. According to the Bitkom survey, former employees are the most important group of perpetrators, representing 60%.

Perpetrators: employees are the greatest risk for know-how



Basis: All surveyed industrial companies affected by data theft, industrial espionage or sabotage in the past two years (n=349). Multiple responses in percent.
Source: *Bitkom survey "Wirtschaftsschutz" ("Economic protection") (2016).*

The Bitkom survey makes clear how varied the motives for industrial espionage, sabotage and data theft can be. The potential perpetrators also include groups that are closely associated with a company – such as its own (current) employees, as well as cooperation partners.

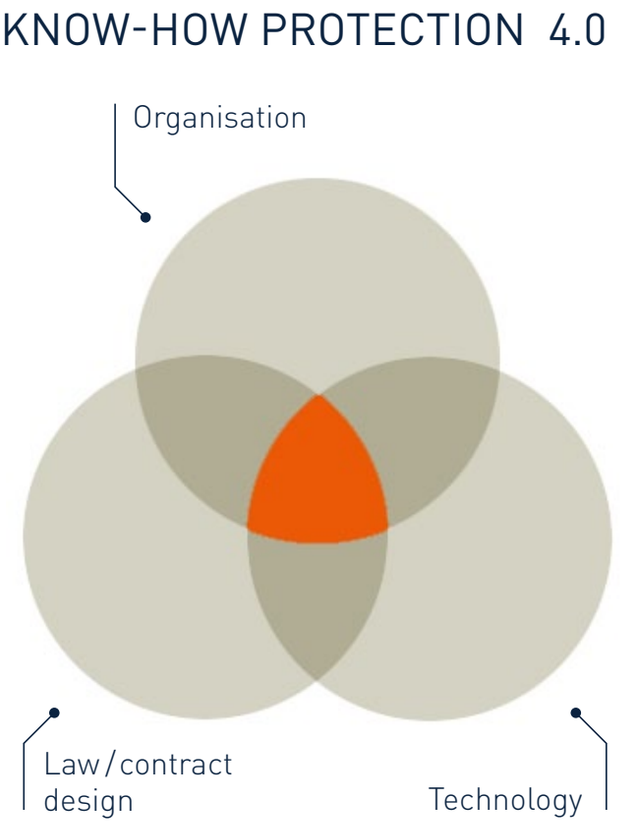
However, in the age of Industry 4.0, trade secrets can no longer be kept on paper under lock and key in a safe. The digital era is dominated by a knowledge society, which derives its advantages from communication using electronic media. In these ecosystems, industrial companies have to anchor know-how protection strategically in order to protect themselves effectively against industrial espionage and data and know-how theft. In other words, there is a huge need to take action in order to achieve improved know-how protection.

Measures for know-how protection

Organisation, contract design and technology are the foundations for the protection of secrets

Industrial companies have to change. In the fourth industrial revolution, they can use intelligent machines and products to optimise their business processes along the whole value chain. In order to turn themselves from product-centred manufacturers to service-oriented service providers with digital business models, they have to become faster and more agile. However, there is one thing they have to preserve: ***their know-how****.*

This is because advances in digital networking simultaneously harbour additional dangers for trade secrets: the more employees in a network that have access to know-how, the greater the danger of conflict relating to existing rights, as well as the risk of unauthorised access by third parties. In the era of Industry 4.0, protection for know-how can come only from a triad of organisation, law (contract design) and technology.



In companies, know-how protection is one of the most important topics in the age of digitalisation. This is the conclusion of a report on the legal challenges of Industry 4.0 produced by Noerr on behalf of the Federation of German Industries (Bundesverband der Deutschen Industrie, BDI).

Industry 4.0 – Legal challenges of digitalisation

Input for the public debate

Organisation

Defining strategically important know-how and taking measures to categorise relevant information and holders of secrets are the foundations for safeguarding trade secrets

Definition

Know-how exists everywhere in a company, but it does not have the same significance for business development in every place. Therefore, those secrets that are especially important for business models have to be defined and protected with particular care.

Measures

Organisational precautions and the categorisation of information form the foundation for contractual know-how protection arrangements and for safeguarding secrets by technological processes.

These include:

- central know-how management, which systematically registers and, where appropriate, categorises both the relevant trade secrets and the holders of know-how
- systematic labelling of confidential information
- clearly defined processes for handling trade secrets and appropriate training courses for employees who come into contact with important know-how
- clearly defined responsibilities and access authorisations
- documentation of the transfer of know-how, and the withdrawal of access authorisations when employees leave the company or individual projects
- documentation of confidentiality measures
- documentation of the disclosure of confidential information to cooperation partners

Law / contract design

Contractual arrangements also form the foundation for know-how protection in the context of digital business models

In digital manufacturing processes and in production with customer participation, the danger of unauthorised access by third parties grows, because a larger group of participants is often involved. As far as possible, therefore, know-how has to be safeguarded contractually.

To protect trade secrets, optimised wording is important in

- contracts with employees
- contracts with cooperation partners / suppliers
- contracts with customers / terms and conditions

Experience in companies shows that it is their own employees, in particular, who can present a risk to trade secrets. Moreover, there is a fear that an employee could take know-how with them in the event of a possible move to a rival company. Especially when it is in digital form, know-how can quickly fall into unauthorised hands. Therefore, it is crucial to incorporate confidentiality clauses, which are as comprehensive as possible into employment contracts. Nevertheless, these clauses must be worded in a sufficiently balanced way, so as to ensure they are effective. This also has a positive practical effect: the employee will take more notice of a stipulation that draws attention to particularly sensitive know-how in the company, gives details about handling secrets and sets out exceptions than they would of a brief three-liner. A meaningless catch-all clause would probably do little to perform the alarm function that is so important in preventing the negligent disclosure of secrets.

If cooperation partners are able to access trade secrets during work on projects, it is very important to have know-how protection clauses in cooperation contracts that are geared to individual cases. The scope and period of validity of the clauses, in particular, are important to avoid pitfalls. Know-how worth protecting that arises as a result of the cooperation must also be borne in mind.

Confidentiality commitments in terms and conditions (T&Cs), in numerous constellations, form a good foundation as a standard in relation to customers. Here, the fundamental risk is that parts of the T&Cs are inappropriate and, therefore, ineffective – for example, because they are one-sided or in relation to the duration of the confidentiality commitment or the contractual penalties specified for breaches of contract.

If you do not protect your know-how appropriately, you are no longer deemed worth protecting in law.

Sandra Sophia Redeker

The new EU Directive on the protection of trade secrets

In April 2016, the European Parliament approved the Directive on the protection of undisclosed know-how and business information against their unlawful acquisition, use and disclosure. The aim is a uniform protection standard across Europe and a common understanding of trade secrets within the European Union.

What does the new Directive mean for companies in Germany? As soon as the Directive has been incorporated into German law, two effects are to be expected:

- Companies will have a wider range of grounds available to them for making claims against infringers
- Companies will have to meet higher standards to be able to take advantage of legal protection for their know-how

Sandra Sophia Redeker, Rechtsanwältin, Associated Partner and Member of the Intellectual Property & Media Practice Group at Noerr, explains how companies can prepare themselves for this.

When will the new Directive on the protection of trade secrets apply to German companies?

The Directive came into force with effect from 5 July 2016 and has to be incorporated into national law by the member states within two years. Consequently, the new legal position will apply from 5 July 2018 at the latest, or earlier, depending on when it is incorporated into national law by Germany's lawmakers. Regardless of this, however, companies should already start preparing for the new rules now and review their existing measures to protect secret know-how and confidential information. Waiting until the rules have been incorporated into national law could lead to a loss of rights in subsequent infringement proceedings.

What is the difference compared with the old legal position?

One substantial change concerns the definition of trade secrets. In future court infringement proceedings against third parties, the holder of the secret will have to explain and prove that he took appropriate

measures in the past to protect his secret know-how and confidential information. This applies not only to legal safeguards but also to organisational measures and IT security standards in the company. If you do not protect your know-how appropriately, you are not deemed worth protecting in infringement proceedings. The fact that proof has to be supplied for the past is a reason why German companies should already be checking their level of protection and eliminating gaps in that protection now.

What else will change with this Directive?

There are also new exceptions for the use of trade secrets by third parties. This means that, in future, reverse engineering, meaning the backward analysis of products that are freely available on the market, will, in principle, be permitted in Germany. Companies should protect themselves as far as possible against reverse engineering through contractual arrangements with cooperation partners and customers.

There is positive news about legal consequences: in future, in addition to prohibitory injunctions, rights to information and claims for compensation, holders of secrets will be able to assert claims for the recall and destruction of infringing products. Finally, the holders of secrets will in future be safeguarded by new rules that are to be created to protect secret know-how in infringement proceedings. The aim of this is to prevent the holder of the secrets having to fear that, as a result of his pursuing court proceedings against infringers, further secret know-how will flow to the infringer or to other third parties because of the fundamentally public nature of the proceedings. Unlike Germany, other countries have long had appropriate protection regulations in this regard. This is an area where we have a serious amount of ground to make up and a lot of adjustments to carry out.

> It is essential to examine the current level of protection in companies.

How can companies prepare for the future legal position?

It is essential to examine the current level of protection in companies, and in every respect. The first condition here is that secret know-how should be captured and categorised according to its significance to the company. Even this often does not happen, especially in small and medium-sized enterprises.

Then, existing protection mechanisms need to be checked for gaps, and this must be done across the operation. To make such risk analysis easier, we have developed a matrix for our clients. This poses the relevant questions for a company's internal affairs and external relations in the three appropriate areas of organisational, legal and IT security measures.
This is just one example from the contractual field. Here, existing rules relating to employees, cooperation and licence partners, customers and suppliers should be examined. This includes checking the effectiveness of contractual provisions, because if a contractual provision is ineffective, it is no more appropriate as a confidentiality measure than a situation in which there are no contractual safeguards at all. Consequently, it is important to use contractual provisions that are as far-reaching as possible and, at the same time, balanced. It is not always easy to separate these two things, partly because of Germany's stringent controls on T&Cs. Technology-intensive sectors should also keep a close eye on reverse engineering as an issue and, where appropriate, define additional provisions in their contracts.

In addition, existing IT measures for protecting secret information need to be checked. This applies, first, to protection against attacks on the IT system from outside and, second, to access to secret information within the company.

What impact will the Directive have on business models – especially digital business models?

Especially for digital business models, it goes without saying that greater attention needs to be paid to the protection of secrets. This applies, first, to the field of IT security. For instance, a Bitkom survey found that three out of four German companies, on average, are exposed to attacks on their IT systems, which cause losses totalling 6.5 billion euros a year. Also, although many companies are certainly aware of their existing security shortcomings, only half of them have an IT emergency management system, for example. In the future, such negligence will not only result in the actual loss of know-how but will also have a negative effect on a company's legal protection. Also, the growing number of players involved as digital business models develop means it is becoming harder to assess situations of risk. The important thing here is to identify and safeguard the numerous sensitive areas for potential loss of know-how.

Technology

Technology is essential for properly safeguarding your trade secrets

Know-how cannot be protected by contractual arrangements alone. Under the new EU Directive on the protection of trade secrets, technological measures will be essential for legal measures against data thieves.

The protection of trade secrets requires, in particular, that...

- data is protected against being accessed from outside (hackers)
- internal access authorisations are granted carefully and reviewed regularly
- data on mobile devices is encrypted

Dr Tobias Bosch is Rechtsanwalt, Partner and Member of the IT, Outsourcing & Data Privacy and Telecommunications Practice Groups at Noerr. He explains what needs to be borne in mind in the use of IT security to preserve trade secrets.

How well can trade secrets be protected by technology?

Companies usually have no interest in asserting their trade secrets in public court proceedings. Court disclosure requirements mean that parts of the secret, at least, often have to be revealed. Therefore, preventive avoidance of the unwanted disclosure of know-how is important. Technological IT security measures are an indispensable component of a protection concept here. They can protect against hacking, espionage or sabotage. Internal risks, too, such as undocumented access to sensitive data or the unintentional importing of viruses or Trojans, can be avoided with technology.

Can this be regulated by technology alone?

For optimum protection of secrets, technological protection measures have to be accompanied by organisational steps. For example, the technological documentation of access to sensitive

documents makes sense only if a company ensures that the necessary access rights are granted restrictively, that access is monitored regularly and that employees always work using their personal ID.

What is it particularly important to bear in mind here?

It is important that risk analyses are carried out regularly to check that the IT security measures are appropriate. It is useful here, for example, to categorise sensitive operational data according to their significance and likely risk potential, with access rights determined on that basis. In addition, protection measures must always be adapted to keep up with current technological requirements. Both hardware and software must be regularly maintained and replaced or updated. In view of the ever-increasing diversification of workplaces and working tools, companies need to think not only about their internal networks, but also about data processing on mobile devices and remote access by employees' private devices, as well as outsourced IT services.

What risks are there if companies carelessly fail to take protection measures?

If protection measures are not taken, there is a danger that the trade secret will be lost to a rival. Depending on its economic importance for the business model, this loss can mean huge damage to the company's value and even endanger its existence. The dimensions of the potential damage are growing with the continued spread of Industry 4.0. The increased networking of machines enables attackers to access production facilities directly. In this way, German companies, in particular, as they are often leaders in technology, can be robbed of their company secrets or fall victim to acts of sabotage. If malware gains access, this can bring the whole production process to a standstill. To improve the protection of networked industrial facilities against cyber-attacks, companies, universities and research establishments have come together and established the National Reference Project for IT Security in Industry 4.0. The aim is to develop methods that will minimise points of attack for hackers and allow for secure data processing in networked facilities.

What has to be borne in mind with regard to liability?

Guaranteeing IT security is already a management responsibility. Therefore, a company's top executives are obliged, as part of the appropriate running of the business, to ensure the basic principles of information security – meaning the confidentiality, availability and integrity of IT systems – and to defend the company against the risks of IT use. This obligation can include internal security guidelines, in addition to the duty to provide the necessary security infrastructure in hardware and software. It can also be wise to appoint somebody with specific responsibility for IT security. Under the new EU Directive on the protection of secrets, claims against infringers will be deemed to be justified only for information that has truly been protected, and in a manner that is legally appropriate. If these claims are rejected because of failure to take appropriate protection measures, the liability risk for the management will be high.

Conclusion

It is becoming harder and harder to protect secrets in the increasingly networked structures of the digital economy. However, safeguarding data, algorithms and software against theft and unauthorised access is essential for every company. As a strategic asset, this know-how is the foundation of digital business models and, therefore, of existential importance for competitiveness in the markets of the future.

Consequently, the strategic safeguarding of digital business models begins with the identification of key know-how. A central management system for trade secrets that captures both the information worth protecting and the holders of that knowledge forms the organisational basis for the preservation of know-how.

For this protection, the professional drafting of contracts with the holders of secrets inside and outside the company is just as crucial as the development of technological barriers to prevent unauthorised access. A risk-management system must, in considering sources of danger, bear in mind not only hacking attacks from outside but also the company's own employees, as well as the staff of suppliers, customers or cooperation partners.

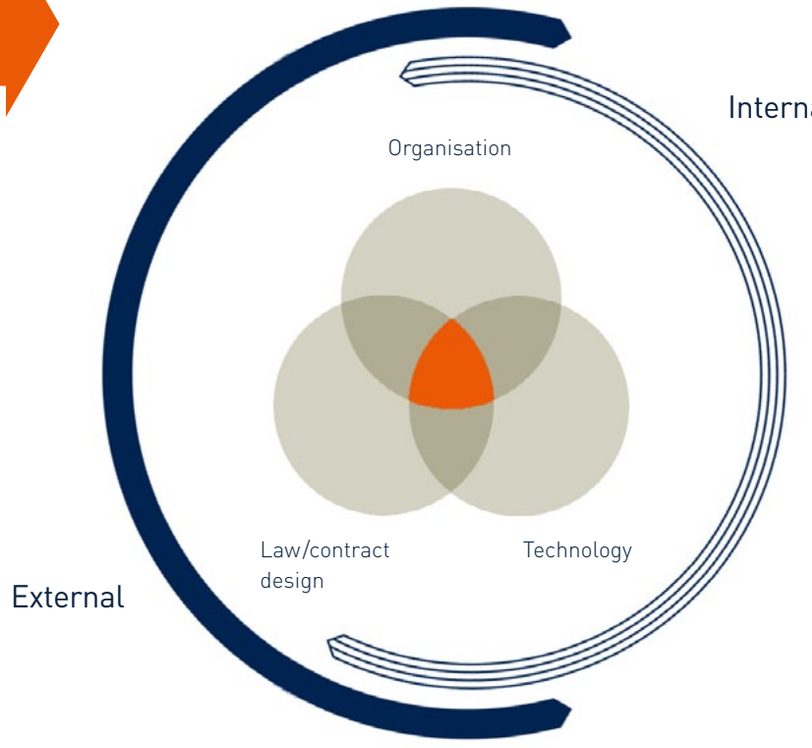
Ultimately, it is important to document know-how protection in detail, so that a company can assert its claims – including through the courts – in the event of the misuse of secret data. For this reason, highly professional solutions are the precondition for the strategic safeguarding of digital business models, in organisational as well as in legal and technological terms.

Noerr know-how protection

With our consulting model, companies can systematically identify and close gaps in their protection

Analysis
- Analysis of existing know-how and secret information
- Identification of gaps in protection

Evaluation
- Evaluation of risk potential
- Assessment of existing risks



Protection/prevention
- Observation
- Measures to prevent (further) risks

Action
- Closing gaps in protection and taking measures to reduce risks

Your point of contact

Sandra Sophia Redeker
Rechtsanwältin
Associated Partner
Practice Group Intellectual Property
& Media

T +49 30 20942069
sandrasophia.redeker@noerr.com

Noerr LLP
Charlottenstrasse 57
10117 Berlin/Germany

About Noerr

Noerr stands for excellence and entrepreneurial thinking. With teams of strong characters, Noerr finds solutions for complex and demanding issues. United by shared values, the 500+ advisors at Noerr have one goal: the client's success. Listed groups, small and medium-sized enterprises and financial institutions and investors trust the law firm's advice.

Entrepreneurial thinking

Noerr's advisors make their clients' challenges their own. They do not only think with them but also think ahead. In doing so, they are at liberty to make their own decisions, and they assume responsibility. Noerr is committed to always going the extra mile for its clients and to resolving complex matters with experience, excellence and sound judgement.

Innovative solutions

In complex and dynamic markets new approaches are regularly required – and delivered by experts who bring both the know-how and the necessary passion. This is what Noerr excels at: implementing integrated and innovative solutions efficiently.

Global reach

In order to be truly able to stand up for its clients without boundaries, Noerr, as a leading European law firm, is also well established internationally, with offices in eleven countries and a global network of top-ranked "best friends" law firms. In addition, Noerr is the exclusive member firm in Germany for Lex Mundi, the world's leading network of independent law firms with in-depth experience in 100+ countries.

Expert in Central and Eastern Europe

Noerr has long had its own offices in all major Central and Eastern European capitals. The firm regularly advises German and international investors on greenfield investments, joint ventures, acquisitions and divestments in Central and Eastern Europe. With around 100 professionals, Noerr is one of the leading law firms in the region.

Noerr Group

Noerr LLP – Noerr Consulting AG – TEAM Treuhand GmbH – NOERR AG Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Offices

Alicante, Berlin, Bratislava, Brussels, Bucharest, Budapest, Dresden, Düsseldorf, Frankfurt, London, Moscow, Munich, New York, Prague, Warsaw

Alicante
Berlin
Bratislava
Brussels
Bucharest
Budapest
Dresden
Düsseldorf
Frankfurt
London
Moscow
Munich
New York
Prague
Warsaw

noerr.com