

Recommendations:

- Identify sensitive know-how of your company.
- Analyse who has access to such know-how inside and outside your company.
- Make sure that the transfer of know-how is included in your security concept.
- Prevent any unauthorised sharing of know-how with third parties by imposing confidentiality obligations and individual agreements.
- In case of business relations, make sure that your partner applies adequate security guidelines.

Please contact us and make an appointment for confidential awareness talks.



Your points of contact

www.verfassungsschutz.de
www.verfassungsschutz-bw.de
www.verfassungsschutz.bayern.de
www.verfassungsschutz-berlin.de
www.verfassungsschutz-brandenburg.de
www.verfassungsschutz.bremen.de
www.hamburg.de/verfassungsschutz
www.verfassungsschutz.hessen.de
www.verfassungsschutz-mv.de
www.verfassungsschutz.niedersachsen.de
www.mik.nrw.de/verfassungsschutz
www.verfassungsschutz.rlp.de
www.saarland.de/verfassungsschutz.htm
www.verfassungsschutz.sachsen.de
www.mi.sachsen-anhalt.de/verfassungsschutz
www.verfassungsschutz.schleswig-holstein.de
www.thueringen.de/de/verfassungsschutz

Imprint: BfV (German federal domestic intelligence service)
for the intelligence services
of the Federation and the federal states

Pictures: © Fotolia.com
© Nikolai Sorokin - Fotolia.com

Print: INFOX GmbH&Co.
Informationslogistik KG, Troisdorf

DOI: August 2010

Domestic intelligence service

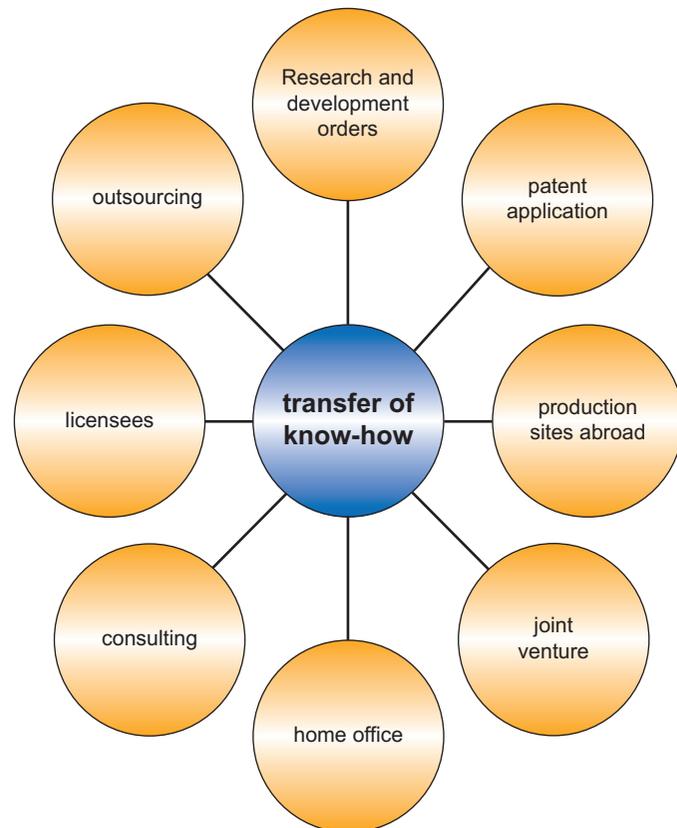


Federal Republic of Germany
 **Federal States**

Security in the transfer of know-how

**Transfer of know-how:
A question of trust**

These days, the risks of unintentionally losing know-how are as manifold as the demands to transfer your own expertise in the course of everyday business processes:



Possible reasons for a transfer of know-how:

- international business activities
- high level of specialisation
- pressure of rising costs
- provision of mobile workplaces
- research and development orders
- leasing and maintenance of information and communication systems

Risk scenarios

As soon as you use a business partner's services, you transfer a part of your know-how to third parties or how to access your data bases. Is your partner trustworthy enough for that?

A medium-sized company tasked a research institute with the further development of a product. Due to an inadequate security concept, a guest scientist could steal know-how and sell it as his own idea.

A German patent attorney's office clerk of a provided a foreign intelligence service with confidential documents.



A car manufacturer commissioned the order to develop a user interface for the on-board computer of a new model. To this end, the manufacturer transferred technical data and specifications of the prototype to a software company with an insufficient security structure. For instance, design plans were openly accessible, and the cleaning staffs were not supervised during their work in the company.

A foreign joint venture partner deliberately exploited the know-how of a German company for simultaneously setting up an own enterprise with an identical range of products.