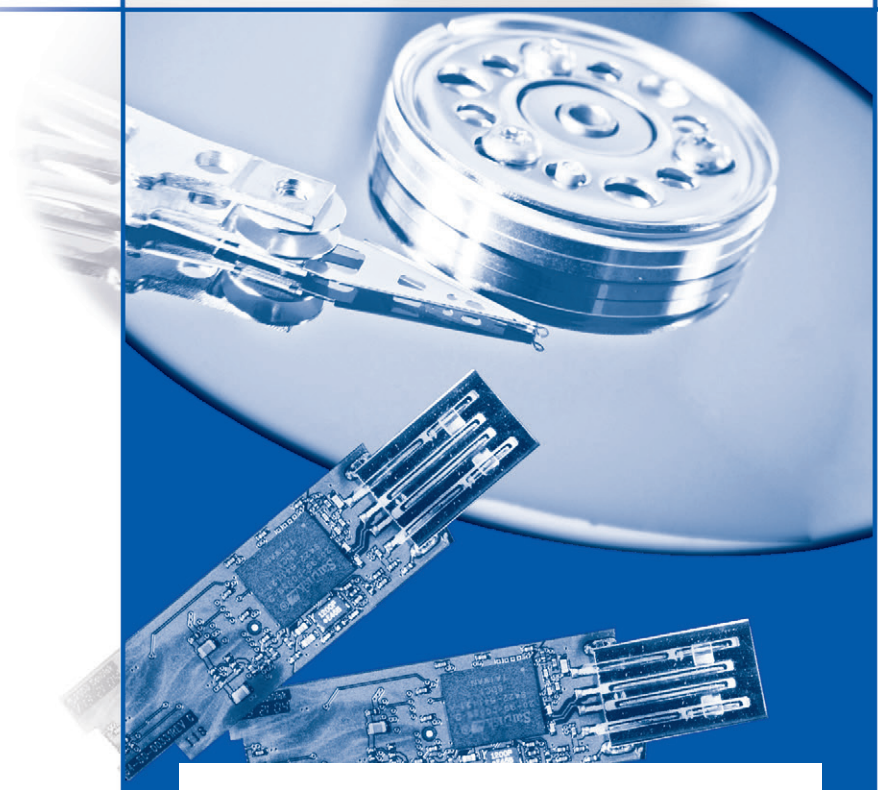

§ 1 Definitions
INFORMATION shall be any confidential information orally, in writing or in any other medium regarding the area refferred to in the Recitals. This shall include, but shall be not limited to data, drawings, designs, drafts, sketches, plan, descriptions, specifications, measurements, results, calculations, experience, methods, processes, samples, models, specific technical knowledge, prodedures and transactions including secret know-how and any applications for any property rights not yet published.

§ 2 Pledge of Confidentiality
The Contracting Parties undertake to hold confidential and all INFORMATION, and not to disclose such INFORMATION, and in whatever part of third parties. The contracting parties undertake to take the necessary steps to prevent third parties from obtaining knowlegde of such INFORMATION, in particular, the contracting parties undertake to provide access to such INFORMATION only of those employees to be obligated to observe this pledge of confidentiality.
The pledge of confidentiality shall also apply also to group companies, licenses or third parties.
If one party wishes to give over INFORMATION to companies affiliated with PARTY, PARTY shall inform the other party prior to disclosing INFORMATION, and shall ensure that those affiliated companies agree to what theprovisions set forth in this Non-Disclosure Agreement.

§ 3 Exclusions from the pledge of Confidentiality
This pledge of confidentiality shall not apply if it can be established that INFORMATION

CONFIDENTIAL

dataEx

Securely Delete and Format

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 Munich

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

info@itWatch.de
www.itWatch.info

dataEx

– Securely delete and format

dataEx enables you, to securely delete any information (files or entire folders) on removable media (flash storage technology) AND hard disks (magnetic storage) or to securely format entire media (including rewritable optical media).

Threads:

- The operating system's own delete functions do not delete – they only unblock the reserved space for further use. It's left to chance, if and when the cleared space is really used. Anyway, the data on the storage medium remains readable for everyone, having access to the medium.
- In the case of USB sticks or other removable media the access is particularly easy. The user believes, the data is apparently deleted – but nevertheless trespassers may get hold of it, without anybody noticing or having done anything wrong.
- A PC storage medium is given to a service provider for maintenance or "repair" – that is for example warranty claims or the clarification of technical problems. Confidential data has been deleted, but not securely deleted.

Challenges:

- For certain data companies are obliged by law to take the technically feasible measures for data protection - including deleting securely. Legal liability is with the executive management/board of directors and can NOT be delegated to others, even if they perform certain actions by order.
- For your own interest you should protect your financial, development and other confidential data against espionage and unwanted uncontrolled access, even beyond the active life cycle of the information.
- It is recommendable (for certain environments mandatory) to comply with the requirements of the BSI for "secure delete" of information worth protecting.

dataEx by itWatch is the Perfect Solution For SMB And Enterprise

The module **dataEx** allows a **secure Delete** of files and folders and their metadata on the basis of the existing permissions, in a way, that even with the best forensic tools they cannot be restored anymore.
In addition **secure Format** makes it possible to securely format existing storage media (also rewritable optical media), so that none of the previously stored data is there anymore.

Both functions can be used in two ways according to your liking:

- The context menu of the data medium, of the folders and of the files in question respectively of the data medium to be formatted contains the entries "Secure delete" respectively "secure format of the data medium". Just click on the function you want to use.

- Alternatively for secure deleting of files and folders by drag & drop you can use on your desktop the drop-target symbol "itWESS shredder". It can also be used for securely formatting removable media.

After each action you get a success respectively failure message on the execution.
All the procedures are compliant with international standards and the requirements of the Federal Office for Security in Information Technology (in Germany: BSI).
Cost reduction: due to this procedure you can use cost effective ways of disposal for your hard disks and mobile storage media – even if they have to comply with legal regulations.

FSdE-270213en