

Data sealing - effective solution to prevent misuse

99% safe data transfer and cloud storage



sealed solutions
GmbH

Otto-Lilienthal-Straße
36
71034 Böblingen

E-Mail
n.bacher@
sealedsolutions.com

www.
sealedsolutions.com

A software concept hardly known to date offers many benefits for digital transmission of electronic data or sharing of files: IRM, Information Rights Management, is the specific assignment of permission to access company data. The application of IRM software provides specific data sealing which can be designated individually and is uncomplicated. sealed solutions GmbH, founded in 2006 and based in Böblingen in Baden-Württemberg, specialize in a whole range of such useful software products.

Collaboration with suppliers, business partners and distributors inevitably entails the supply of valuable and often confidential information. Online access to files, databases, graphics or videos is taken for granted and this cost and time saving method has to be maintained. But how can it be ensured that data is accessed by authorized persons only and within the agreed scope and period? The laptop used on a train, the smartphone left out of sight for a moment during a conference break or the loss of a USB stick pose a huge risk and can turn into a nightmare. These devices often contain comprehensive company, product or personal information, the loss of which can cause massive damage to the company's image and financial loss once the information falls into the wrong hands accidentally or intentionally. But how can misuse be prevented? There is also a large number of unreported cases of former employees using unauthorized copies of company data to cause immense damage. What precautions can be taken to ensure that valuable data is or becomes unusable in such cases?

Regardless of the file format or the system software, IRM products seal the data and assign the respective roles and permissions to users. Norbert Bacher, managing director

at sealed solutions GmbH, describes the daily operations of IRM: "The respective usage permission can be assigned to each file or, alternatively, to predesignated user groups individually. Unknown users are definitely prevented from using sealed data. Thereby blunder or manipulation can be excluded." The 55-year-old sales manager and IT specialist knows the risks he is talking about. He has 5 years of experience in sales and key account management in the international food industry. "I know now what kind of success sealed data would have been in those days. Many a product idea would not have fallen into the wrong hands, i.e. the hands of the competition. Data theft by internal or external users could have been prevented. Not to mention data forwarded by mistake when sending urgent emails," says Bacher regarding his experience prior to sealed solutions. The team of thirty IT experts at sealed solutions GmbH and their partners advise customers on the requirement for basic or additional data security. Installation, maintenance and user support are as much a part of customer care as is the training of company IT decision makers and users.

How to prevent the risk of data loss and manipulation

Data sealing makes it possible – independent of the file format – to assign specific rights to certain authorized users with regard to the extent, period or exact time of usage and also which PC, smartphone, tablet PC or data carrier may be used. The specified rights can be modified, revised or revoked by IRM (Information Rights Management) at any time. Thus sealed data is effectively protected against misuse inside and outside the company.

IRM Software security provides additional

convenience: the assigned rights are administered separately from the sealed data on a separate server. Thusly, sealed solutions ensures that, in case of an attack, sealed documents can never be stolen together with the user rights. Unauthorized modifications to or removal of allocated rights are therefore impossible.

Implementation in the food industry

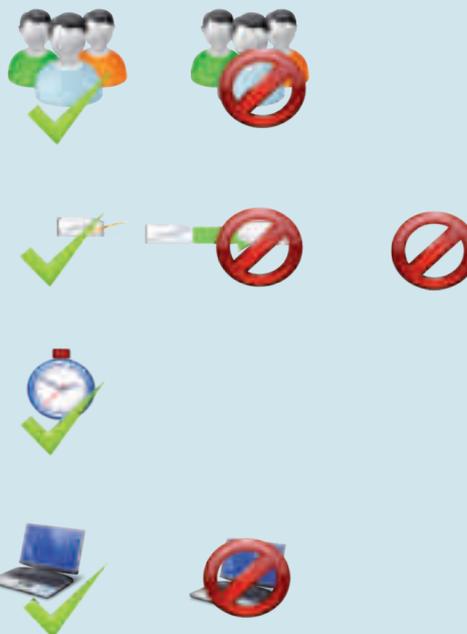
Before sending a product specification for a new confectionery product to a potential supplier of ingredients, the use of IRM-Software can restrict access to the extent that the file can only be opened at the workstation of the respective email recipient. Due to data sealing it is not possible to print, save or forward the file. The marketing plan for the launch of a new product range, destined to be sent to a marketing agency, is sealed for viewing once only as a basis for a quotation, only for the duration of one hour during the project meeting and exclusively on a computer screen.

The information contained in a customer database can only be accessed by field staff or representatives with a designated terminal device. Data sealing will also prevent the data from being misused if the contract with the sales partner is terminated.

A subcontractor is given the file with a recipe for a new product, a file which comes with limited access rights regarding saving or reading of data. As soon as the recipe or the agreed co-operation terms and conditions with the supplier are revised, permission for the usage of the file can be revoked or updated. This ensures a very high safety standard and the effective compliance with quality standards even in the case of product liability.

Basic checklist for data sealing

- **WHO (authorised user)**
Persons and groups inside and outside the company
- **WHAT (permitted use)**
Reading, editing, circulation or printing rights
- **WHEN (right time)**
Time limits, date, period, duration
- **WHERE (right place)**
Certain IP addresses or certain places



IRM solutions provided by sealed solutions are also appropriate for mobile devices. The permission to access electronic information stored on a USB stick or smartphone when travelling abroad can be assigned for a limited period of time and for the specific data carrier only. If the data carrier is lost, data sealing prevents misuse.

Data sealing is more than data security

According to a PwC AG survey the crime rate concerning customer and business data in Germany has increased from 12 to 21% since 2009. Data theft ranks high in

the statistics, right behind offences against property and infringement of intellectual property rights. The loss, theft and resulting harmful usage of data do not only lead to substantial financial problems for a company. The entailing damage to the reputation with regard to customers, banks, the public and media has a negative long-term effect on the success and the market position of managers, companies and products. Numerous data security problems of international companies that have become public show the shattering effect of such incidents.

As a result of such risks, quality man-

agement procedures and quality certifications will put more and more emphasis on complex data security. Future business partners, shareholders and customers with certified diligence and pre-emptive company activities will have superior quality and an advantage over the competition. "The protection of information is also the protection of investments!" is Bacher's motto for his customers. Furthermore, the verified use of IRM to seal data is an important legal instrument in connection with data protection or in case of copyright and intellectual property rights claims.