



# Deutsche Telekom AG– – Brainloop Secure Dataroom as a collaboration tool for Corporate Communications

## FAST FACTS:

- CUSTOMER:**  Deutsche Telekom AG, Corporate Communications, Bonn / Germany
- CHALLENGE:** Unsecure email and fax communication and unprotected data transmission by disk
- SOLUTION:** Brainloop Secure Dataroom provides a platform for planning and preparation of the annual DTAG stockholders meeting and enables implementation of publication projects.
- BENEFITS:**
- Simple integration of external service providers
  - Eliminates unsecure and unnecessary email traffic
  - Project Manager can act as the Dataroom Administrator
  - Provides a document management system
  - Provides secure document archiving
  - Enforces high security levels with token-based authentication (SMS)

The Corporate Communications department at Deutsche Telekom AG has been working with Brainloop Secure Dataroom™ for just over a year. The web-based dataroom has proven itself to be an efficient, collaborative working platform for documents that frequently have to make the rounds, particularly in this division where projects often involve many external participants such as agencies, service providers, and freelance journalists.

André Staudt, Technical Internet Project Manager for Corporate Communications at DTAG, explains: "Everyone in Corporate Communications that is involved in a specific project has completely secure access to the confidential project documents via the Internet." They receive informative email messages about relevant procedures in the dataroom, they can edit files, and the dataroom is used to communicate with others involved in the project. For instance, one can open a "discussion" in the dataroom and others can check the audit trail to understand who has already seen or edited which file. Staudt adds, "The

particular advantage of a web-based dataroom is that it is so incredibly easy and uncomplicated to use. The project participants need practically no training time and there is no implementation effort with external project partners either. Highly distributed project teams with external project members particularly benefit from this cross-company, highly secure working environment."

Brainloop Secure Dataroom allows numerous people to edit confidential business documents at any time from any location via the Internet. Provided they are authorized to do so, users inside or outside the company can access the dataroom, or – depending on their authorization – may access only individual documents stipulated for them. Daily activity within the dataroom is very simple to transact. The user authenticates from any location via a web browser with a user name and a user-selected password. To prevent manual or automatic testing of passwords and tokens, failed attempts are logged along with the IP address and can be viewed by the application administrator at any time. After a certain number of

## Deutsche Telekom AG – Brainloop Secure Dataroom as a collaboration tool for Corporate Communications



failed attempts, a user account is blocked for a period of time. Token-based authentication provides an additional level of security, either for the entire dataroom or for individual parts of the dataroom. Here Brainloop has creatively solved the problem of token usage: the user's mobile phone is simply the token. A single session PIN is sent by flash SMS to the user's telephone number.

"In the search for a secure collaboration tool, it soon became clear that there was really no alternative to Brainloop's secure dataroom with regard to functionality, security, and user friendliness," says André Staudt about his decision to choose Brainloop's virtual dataroom. "Over 100 people work with our dataroom, about 90 percent of them within our Corporate Communications division. Approximately 10 percent of the users are external project partners. Today we transact the majority of our Corporate Communications projects with the Secure Dataroom," says Staudt. "This includes technical projects, such as the planning and preparation of the DTAG annual stockholders meeting, publication projects, data exchange for creating print media, and the publication of our employee magazine or newsletters.

"A huge advantage of the web-based dataroom is that external agencies, graphic designers or journalists can easily be integrated. This prevents a great deal of unnecessary, and potentially unsecure, email traffic", adds Staudt. Individual access rights can be defined not only for individual datarooms or dataroom directories, but even down to the level of individual files.

"Administrators set up datarooms and allocate the access rights for different projects," explains Staudt. "Our dataroom administrators can be myself, a colleague or individual project managers. Project managers define project milestones within their dataroom and stipulate who is to be informed about what procedure at what time. They also allocate roles to project members and therefore designate editing rights. Project managers also post their status lists in the dataroom. Central planning documents such as this are often highly protected. These documents may be read by the other project members, but not edited. This allows the project manager to defines

the authorizations linked with the document accordingly," Staudt explains. "It does not take long to learn the administrator functions. Any project manager can quickly learn how to set up a dataroom without any special IT knowledge. Brainloop also provides both onsite or online training for new users.

Initially, a company must define a document archiving structure, as well as the associated user groups, roles, and authorizations. Thanks to various dataroom templates, which a company can select according to its needs this is done quickly and efficiently. Once a specific company dataroom template has been generated, it can be reused again and again to generate specific datarooms for diverse projects within a company's dataroom center – each with a distinct encryption key. The Secure Dataroom service can be activated and ready for use within three hours.

Brainloop Secure Dataroom not only provides a highly secure, collaborative working environment and acts as a platform for a cross-company exchange of sensitive information, it is simultaneously an efficient document management system that creates an audit trail of every access to a document and records every modification in detail. The dataroom provides a complete version history, an integrated audit trail, and also records each time a document is opened or edited. Each access and modification made to documents, plans and decisions, is logged in detail. Such a feature is especially useful for highly complex editing and sign-off processes. If necessary, the audit trail can also serve to provide revision-safe evidence concerning what information was shared with whom at what time.

"Sometimes the dataroom acts as a document archive for us since one can store large-sized documents

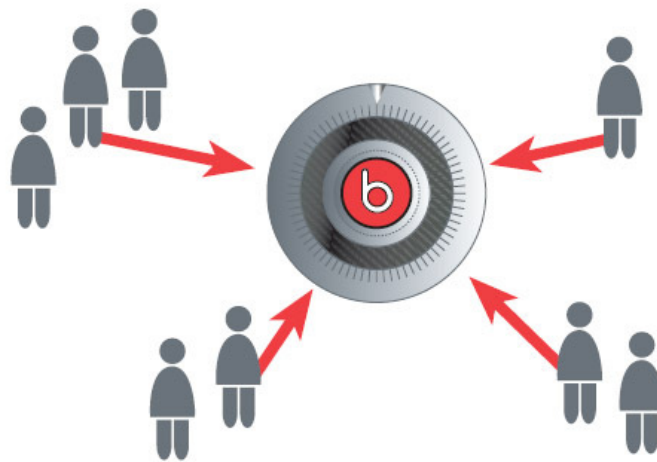
»» In the search for a secure collaboration tool, it soon became clear that there was really no alternative to the Secure Dataroom with regard to functionality, security, and user friendliness. ««  
André Staudt

## Deutsche Telekom AG – Brainloop Secure Dataroom as a collaboration tool for Corporate Communications



there. The maximum possible size for a single file is currently 50 MB. For video streaming, of course, we'd sometimes like 300 MB and are considering an upgrade," Staudt notes, "but 50 MB are also a lot. That's why we also use the dataroom specifically for sharing larger documents. It simply wouldn't be possible by email." The upshot, according to André Staudt, is very positive: "Our

experience with the secure dataroom has been positive for an entire year. It is a secure and highly user-friendly collaboration tool for us. Executing our projects this way has proven to be enormously beneficial for us."



### Security in the Dataroom

Since November 2003, Brainloop has offered an On-Demand version of Brainloop Secure Dataroom in conjunction with T-Systems International (TSI). TSI provides a highly secure datacenter to host the Secure Dataroom service. Not only is the physical security of the Secure Dataroom server ensured, each data transmission to and from the dataroom, (i.e. the upload and download of documents) is also protected with 128-bit encryption. Additionally, all documents stored on the server are powerfully encrypted with 256-bit keys and the recognized "Advanced Encryption Standard" (Rijndael algorithm) so that the dataroom contents cannot be accessed in the T-Systems datacenter where the server is hosted. The encryption and key administration for the operator and users runs transparently in the background and without user input.