

**Q: Nicole, there are many business situations where information needs to be sent back and forth between multiple parties. Examples include establishing a company abroad, holding credit discussions with banks, and conducting due diligence for mergers and acquisitions. The people involved have to read and verify contracts, financial figures and annual reports. Emails with attachments in different versions are sent to and from lawyers, auditors, consultants and external service providers. What can companies do to keep track of all this information?**

A: The examples you mention are typical situations in which highly confidential documents need to be shared and worked on with external business partners. Many companies still do this by email. Yet email is hardly the right solution if they want to protect their sensitive documents from misuse and

from falling into the wrong hands. At Brainloop, we help our customers solve this conundrum by providing a virtual data room – the Brainloop Secure Dataroom – where they can store, share and collaborate on documents while ensuring regulatory compliance. They also have full control over

who does what with a document and when. There's revision control to help users keep track of different versions of a document, and a tamper-proof audit trail that records all communication flows. All this is stored securely in the data room. The Brainloop Dataroom also includes an intelligent permissions system that lets the project manager define what each team member can do with a document – read only, edit it, print it and so on.

**Q. During mergers and acquisitions there's always a risk that potential investors pretend to be interested in buying a company, whereas in reality they're only interested in details of its business strategies, pricing models and market position. It seems like an easy way for confidential information to fall into the hands of competitors. How can a company protect itself against that?**

A. M&A activities are increasingly carried out in the privacy of a virtual data room (VDR). This lets companies assign precise access permissions to each bidder, with exact document rights and restrictions such as "read only" or "all documents must include a watermark". They can also enable or disable forwarding or saving a document on a local PC. If required, access can be limited to a certain period of time. With these functions, companies not only keep control over all their information, but also accelerate the M&A process and make it more efficient and cost-effective.

**Q. Could you give us an example?**

A. Of course. Compliance with rules that stipulate how to handle confidential information – known as DCM for Document Compliance Management – is vital during M&A transactions. But it's also crucial in any business situation where people need to share and collaborate on confidential and sensitive information. One example is the administration and processing of HR data. One of our customers, Fujitsu Technology Solutions, uses the Brainloop Secure Dataroom in their personnel department. Their headquarters and branch offices often need to share personnel files, employment contracts, and other confidential documents. Clearly they need to ensure maximum protection for all the personal information involved.

**Q. Is this type of data room really secure? The media always seem to be reporting spectacular hacker attacks on company networks. If a hacker succeeds in getting into a data room, doesn't he have access to all the documents it contains?**

A. We offer our customers a software-as-a-service option, enabling them to "rent" their DCM solution. So the customer's data is secured on an external server located in a high-security data center. A hacker wouldn't even know where to look for information about the company he's interested in.

Aside from that, security is our core competency. The external data center is ISO certified, and the data centers provide maximum security, backup systems, and the highest availability. We have our data rooms – and the entire technology environment – tested on a regular basis, including for external attacks. These rigorous tests have always convinced our customers, even those with extremely stringent security requirements. The data room is sealed off in accordance with the highest security standards and we have multiple protection levels that even block access by datacenter operators and IT departments. On top of that, all documents are encrypted in storage as well as during uploads and downloads.

**Q. Can companies still use your solution when they have offices in multiple different countries?**

A. Of course, because the information is all stored in the data room – or in the "cloud" as you can read now. So users only need a Web browser, plus a cell phone to receive a message with the password they'll need for authentication. They have fast and secure access to their data room any time and from anywhere with two-factor authentication (user name plus password and a one-time password sent to their cell phone). Several of our customers work with their global offices and partners in the data room.

Nachfolgend das Interview in Deutsch:

**Den Abfluß von Informationen intelligent verhindern**

**complianceforum.de im Gespräch mit Nicole Dietrich, Senior Marketing Director, Brainloop AG, München**  
**Sehr geehrte Frau Dietrich, bei der Neugründung einer Firma im Ausland, bei Kreditgesprächen mit Banken, Due Diligence Prüfungen, bei Firmenkäufen müssen die Beteiligten Verträge, Geschäftszahlen, Finanzberichte lesen und prüfen. Emails mit Anhängen in verschiedenen Versionen werden an Rechtsanwälte, Wirtschaftsprüfer, Berater oder auch externe Dienstleister hin- und hergeschickt. Was kann ein Unternehmen tun, um hier den Überblick zu behalten?**

Sie haben einige der typischen Beispiele aufgezählt, in denen hoch vertrauliche Dokumente gemeinsam mit externen Partnern bearbeitet oder ausgetauscht werden müssen. Und leider geschieht das noch oft mit Hilfe von E-Mails. Um jedoch die sensiblen Dokumente vor Missbrauch oder Fehlverhalten zu schützen, ist E-Mail nicht das richtige Medium. Wir von Brainloop helfen unseren Kunden mit einem virtuellen Datenraum, dem Brainloop Secure Dataroom, in dem sie ihre Dokumente regelkonform ablegen, austauschen, gemeinsam bearbeiten können und noch dazu die volle Kontrolle bewahren, wer hat wann was an den Dokumenten gemacht. Natürlich werden alle Kommunikationsvorgänge im Datenraum voll versioniert und mit Audit Trail (Historie) abgelegt. Zudem bietet der Brainloop Datenraum ein sehr intelligentes Berechtigungskonzept, dass es dem Projektleiter erlaubt, von „Read Only“ bis „Bearbeiten“ oder „Ausdrucken“ sehr gezielt Rechte an die einzelnen Mitglieder zu vergeben.

**Gerade bei Firmenverkäufen besteht die Gefahr, daß potenzielle Investoren gar nicht an dem Kauf des Unternehmens interessiert sind, sondern nur an den Geschäftsstrategien, den Preismodellen und der**

**Marktstellung der Firma. So gelangen geheime Informationen schnell in die Hände von Wettbewerbern. Wie kann sich ein Unternehmen hiergegen schützen?**

M&A, also Kauf und Verkauf von Unternehmen oder Unternehmensteilen wird immer öfter in Virtuellen Datarooms (VDRs) durchgeführt. Man kann so jedem Bieter gezielte Zugangsberechtigungen, genau abgestimmte Rechte (z.B. „nicht ausdrucken“ oder Dokumente nur mit Wasserzeichen ...) einstellen. Ebenso ist natürlich jede Art von Weiterleiten oder Abspeichern auf dem eigenen Rechner abzuschalten. Der Zugang ist zudem zeitlich begrenzt. So behält man nicht nur die Kontrolle, man kann einen M&A Prozess auch effizient, schnell und kostenoptimiert durchführen.

**Können Sie uns bitte ein konkretes Beispiel geben?**

Gerne, der regelkonforme Umgang mit vertraulichen Dokumenten, auch DCM – Document Compliance Management genannt - ist nicht nur bei M&A Transaktionen wichtig, sondern über all da im Unternehmen, wo vertrauliche, sensible Informationen ausgetauscht, bearbeitet werden müssen. Auch bei der Verwaltung und Bearbeitung von Personaldaten. So setzt z.B. die Firma Fujitsu Technology Solutions in der Personalabteilung auf den Brainloop Secure Dataroom. Zwischen der Zentrale und den Niederlassungen werden häufig Personalunterlagen, Arbeitsverträge und andere vertrauliche Dokumente ausgetauscht. Hier muss auf den Schutz dieser personenbezogenen Daten maximaler Fokus gelegt werden.

**Ist so ein virtueller Datenraum auch wirklich sicher? In den Medien wird von großangelegten Hackerangriffen berichtet. Wenn so ein Hacker erfolgreich ist, hat er mit einem Mal Zugriff auf alle Dokumente.**

Wir bieten unseren Kunden die Möglichkeit, auch DCM als Software as a Service zu „mieten“. Das heißt, die Daten des Kunden liegen dann auf einem externen Server, der in einem hochsicheren Rechenzentrum steht. So weiß ein Hacker schon mal gar nicht, wo er die Daten der Firma, an der er interessiert ist, genau suchen soll. Zudem ist dies genau unsere Kernkompetenz, das externe Rechenzentrum ist ISO zertifiziert und beide sorgen so für maximale Sicherheit, Backup-Systeme, höchste Verfügbarkeit.

Wir lassen unseren Datenraum und das technische Environment natürlich regelmäßig testen, auch auf Angriffe von außen. Bis jetzt konnten diese Test all unsere Kunden überzeugen, selbst die, die sehr hohe Ansprüche an Sicherheit stellen. Der Datenraum ist nach den höchsten Sicherheitsstandards abgeschottet und wir haben verschiedene Sicherheitsebenen, die sogar den Betreiber oder die IT Abteilung ausgrenzen. Alle Dokumente sind verschlüsselt, ebenso wie die Übertragung bei Up- und Download.

**Können Unternehmen Ihre Lösung auch dann benutzen, wenn sie Niederlassungen in Deutschland und im Ausland, zum Beispiel in Taiwan haben?**

Selbstverständlich, die Daten liegen im Datenraum – um einen neuen Begriff zu benutzen in „the Cloud“. Das bedeutet, der Anwender benötigt nur einen Internet-Browser, ein Mobiltelefon, für das SMS-Password, das er zur Authentifizierung benötigt. Also kann man von überall, zu jeder Zeit durch eine 2-Faktoren-Authentifizierung (Benutzername, Passwort und Einmal Passwort über das Handy) sicher und schnell auf die Dokumente im Datenraum zugreifen. Viele unserer Kunden arbeiten weltweit mit ihren Niederlassungen oder Partnern im Datenraum.

**Das Interview für [www.complianceforum.de](http://www.complianceforum.de) führte Christian Koch, München**

[http://www.complianceforum.de/index.php?option=com\\_content&view=article&id=16%3Anewstext1&catid=9&Itemid=1](http://www.complianceforum.de/index.php?option=com_content&view=article&id=16%3Anewstext1&catid=9&Itemid=1)

