

## Anwendungsbeispiel Mergers & Acquisitions: Austausch von vertraulichen Firmenunterlagen

### 1) Fallbeispiel

Ein Team von Investmentbankern, Wirtschaftsjuristen, Wirtschaftsprüfer und Beratern arbeitet an der Fusion mit oder Übernahme eines Unternehmens. Das Projektteam muss dabei verschiedene vertrauliche Dokumente firmenübergreifend austauschen und bearbeiten. Ein Projekt läuft über mehrere Wochen bis zu seinem Abschluss.

### 2) Anforderungen

- Gemeinsamer Arbeitsspeicher für Dateiaustausch
- hohe Sicherheit, die den Bedürfnissen der Geheimhaltung entspricht
- möglichst einfache Nutzung ohne Bedarf an Training
- Echtzeitbenachrichtigung über Eingang neuer Dokumente an alle Teammitglieder
- sicherer Nachrichtenaustausch firmenübergreifend
- Zugriff vom PC und auch von mobilen Geräten – Smartphone und Tablet – aus
- einfache Verwaltung – hinzufügen und entfernen von Teammitgliedern
- rückstandsfreies Löschen des Arbeitsbereichs nach Abschluss eines Projekts
- geringe Kosten je Privacy Box
- optional zusätzliche Sicherheit bei der Anmeldung im Dienst.

### 3) Betrachtete Lösungsoptionen

- a) eMail: Dies entspricht der bisherigen Arbeitsweise. Dokumente werden per E-Mail ausgetauscht und jeweils lokal gehalten. Leider muss für jedes Projekt erneut die Etablierung von eMail-Verschlüsselung geklärt werden, die oft nicht firmenübergreifend vorhanden ist. Ein gemeinsamer Team-Arbeitsbereich fehlt. Ergebnis: Anforderungen nicht erfüllt.
- b) SharePoint oder interne Plattform: Hier werden die meisten Anforderungen erfüllt. Es hat sich jedoch als schwierig erwiesen, externen Nutzern den Zugriff auf interne Systeme zu gewähren. Ergebnis: Anforderungen nicht erfüllt.
- c) Öffentliche FileSharing Dienste: Diese Dienste bieten einfachen und bequemen Zugang sowie Nutzung. Leider erfüllen sie zumeist nicht die Sicherheitsanforderungen von Unternehmen. Zusätzlich dürfen geheime Daten und Dokumente nicht auf Systemen gespeichert, wenn der Service Provider prinzipiell auf die Dokumente zugreifen könnte. Ergebnis: Anforderungen nicht erfüllt.
- d) Data-Rooms: Diese Dienste bieten ein hohes Maß an Sicherheit und erfüllen viele der genannten Anforderungen. Die Dienste sind jedoch sehr teuer und erfordern zumeist einen höheren Verwaltungsaufwand. Ergebnis: Anforderungen weitgehend erfüllt jedoch teuer und aufwendig.

### 4) Der Dienst iDGARD erfüllt alle diese Anforderungen

iDGARD erfüllt alle Anforderungen bei sehr geringen Kosten und einfacher Nutzung sowie Verwaltung. Außerdem schließt iDGARD wegen der ihm zugrunde liegenden Sealed Cloud Technologie als einziger Dienst den Zugriff des Service Providers auf die Daten der Anwender aus. Durch die iDGARD Login Card (TAN-Generator im Scheckkartenformat) kann zusätzliche Sicherheit bei der Anmeldung geschaffen werden.

Ergebnis: Optimal, um den Anforderungen gerecht zu werden.

## 5) Konkreter Einsatz von iDGARD

iDGARD Privacy Boxes als sichere Team-Arbeitsräume

### **iDGARD** – sichere Kommunikation und Datenaustausch

#### 1. Sicherer mobiler Aktenkoffer

Jederzeit Zugriff auf Ihre Daten – mobil mit speziellen Apps oder per Browser



#### 2. Alternative zu FTP- & Filesharing-Diensten

Große Dateien sicher versenden – automatisches Schlüsselmanagement – leicht verständlich

#### 3. Projekt- & Team-Arbeits-Räume

Firmenübergreifender Dokumenten- und Datenaustausch, Nachrichten & Chats



#### 4. iDGARD Datenräume

Schutz vor unerwünschter Weiterverbreitung (z.B. Wasserzeichen, Journal,...) für PDFs

Die Registrierung der hauptverantwortlichen Firma bei iDGARD dauert nur zwei Minuten. Anschließend kann man iDGARD sofort online verwenden und kann anderen projektbeteiligten Personen, egal ob intern oder extern, Zugang zum gemeinsamen Arbeitsbereich einräumen.

Der hauptverantwortliche Projektleiter legt dann innerhalb von Sekunden eine Privacy Box für das Projekt an. Insgesamt steht ein Pool mit 100 GB Speicherplatz im Starter-Paket für alle Lizenzen zur Verfügung, innerhalb derer er bis zu 2.000 solcher Privacy Boxen anlegen kann. Weiterer Speicher kann bei Bedarf flexibel und individuell dazu gebucht und sofort genutzt werden.

Sind Funktionen wie Journal, Wasserzeichen oder Dokumente nur zur Ansicht notwendig, lässt sich jede Privacy Box ganz einfach und schnell in einen Datenraum umwandeln.

Die Mitglieder des Projekts, intern und extern, werden vom Projektleiter per Auswahl aus dem iDGARD-Verzeichnis in den Datenraum eingeladen – jeweils mit nur einem Klick.

Allen Ansprechpartnern, wie z.B. Juristen, Berater etc., weist er eine Gast-Lizenz zu, falls diese keinen eigenen iDGARD-Account haben. Dazu wird lediglich die eMail-Adresse und Mobilrufnummer des jeweiligen Ansprechpartners benötigt.

Alle Teammitglieder, intern und extern, nutzen die Privacy Box zum Austausch von Dokumenten und Nachrichten. Die Dokumente werden dabei in entsprechenden Verzeichnissen strukturiert und somit thematisch geordnet für alle Teammitglieder sichtbar gespeichert.

Alle Teammitglieder haben jederzeit per Browser oder App Zugriff auf alle Unterlagen zum Projekt – von Ihrem PC oder auch vom Smartphone & Tablet aus.

Ist ein Projektmitglied längerfristig verhindert oder die Zuständigkeit ändert sich, können Lizenzen jederzeit an inkl. der enthaltenen Boxen an seinen Nachfolger übertragen werden.

Zum Nachrichtenaustausch zw. den Projektmitgliedern verwendet man verschiedene Methoden:

- a) iDGARD Chat für den Austausch in Echtzeit, d.h. sofortige Diskussion online möglich.
- b) iDGARD Notizen für Nachrichten, die für eine Nachverfolgung der Diskussion parallel zu den jeweiligen Dokumenten gespeichert werden.

Nach Abschluss des Projekts wird der Inhalt der gesamten Privacy Box lokal archiviert – und anschließend gelöscht. Dies erledigt iDGARD rückstandsfrei.

Für ein Projekt mit 3 internen Mitarbeitern, 2 Rechtsanwälten und 6 Beratern werden folgende iDGARD-Lizenzen benötigt: 5 x Volllizenz und 6 x Gastlizenz

Jeder Nutzer kann parallel in beliebig vielen Boxen arbeiten, zu welchen er eingeladen wurde.

Generell zeigt sich, dass iDGARD intuitiv ohne Training und ohne Softwareinstallation von den internen Mitarbeitern als auch von den Ansprechpartnern beim Mandanten produktiv genutzt wird.

Kontakt:

Unicon – The Web Privacy Company  
Agnes-Pockels-Bogen 1, 80992 München

[www.idgard.de](http://www.idgard.de) | [contact@idgard.de](mailto:contact@idgard.de)  
Telefon: 089 / 4161 5988 100

