DIGITALE TRANSFORMATION UND IT-SICHERHEIT

Wie Sie Ihr Unternehmen digitalisieren, ohne Cyberkriminellen Angriffsflächen zu bieten

BRAINLOOP

Diligent

Zwei Seiten einer Medaille: Digitale Innovationen und IT-Sicherheit

Liebe Leserinnen und Leser,

infolge der Corona-Pandemie hat die digitale Transformation in vielen Unternehmen einen signifikanten Fortschritt erfahren. Angestellte arbeiten immer häufiger eigenverantwortlich im Homeoffice und Kunden nehmen zunehmend Dienstleistungen via Internet in Anspruch – von Video-Beratungen bis hin zu e-Learning-Kursen.

In diesem Kontext wird umso mehr deutlich, dass viele Entscheider die Krise auch als Chance begriffen haben, ihr Unternehmen zukunftsorientierter auszurichten. Zahlreiche Aufsichtsräte, Vorstände und Geschäftsführer definieren sich inzwischen ohnehin als agile Treiber der digitalen Transformation.

In vielen Chefetagen ist die einstige Tech-Skepsis einem Digital-Optimismus oder gar -Enthusiasmus gewichen.

Zwei Seiten einer Medaille: Digitale Innovationen und IT-Sicherheit

Bei aller Begeisterung für neue Technologien und innovative Geschäftsmodelle sollten sich jedoch Entscheider immer ein grundlegendes Prinzip vor Augen führen: Wer digitalisiert, setzt sich auch digitalen Gefahren aus. Erpressung, Sabotage sowie der Diebstahl von Kundendaten durch Cyberkriminelle sind nur einige ausgewählte Beispiele solcher Gefahren.

Insbesondere Cyberkriminelle birgen potentiell fundamentale Unternehmensrisiken. Unternehmen sind für ihre Kundendaten verantwortlich und im Verlustfalle drohen seit Inkrafttreten der EU-Datenschutzgrundverordnung (DSVGO) empfindliche Bußgelder – von Reputationsschäden ganz zu schweigen.

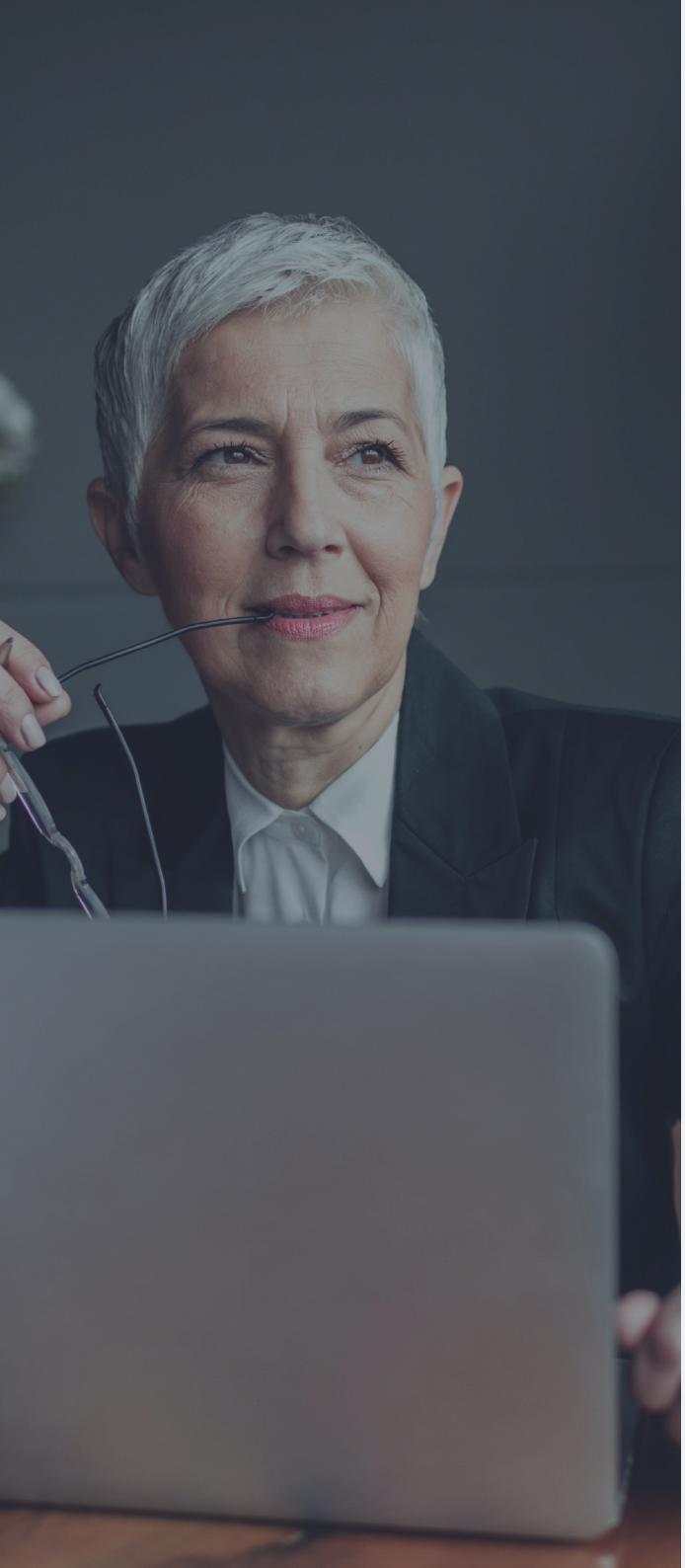
Gute Unternehmensführung im digitalen Zeitalter („Modern Governance“) heißt deshalb, diese Risiken vollumfänglich im Blick zu behalten und sicherzustellen, dass die IT-Sicherheit bei der digitalen Transformation eine hohe Priorität genießt.

Mit intelligenten Strategien und innovativen Tools können Führungskräfte ihre Unternehmen in eine sichere digitale Zukunft steuern. Auf den folgenden Seiten stellen wir Ihnen drei aktuelle Beispiele vor, wie man digitale Herausforderungen mithilfe von hochsicheren Lösungen bewältigen kann.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre. Brainloop als Teil der Diligent-Gruppe und ich stehen Ihnen jederzeit gerne für Fragen oder Anmerkungen zur Verfügung.

Mit freundlichem Gruß

Ihr Ulf Gartzke
(CEO Brainloop)



HERAUSFORDERUNG NEW WORK

Wie vertrauliche Informationen beim mobilen Arbeiten vertraulich bleiben

Unternehmen, die neue Ideen und innovative Geschäftsmodelle entwickeln wollen, setzen immer öfter auf New Work. Das heißt vor allem: flachere Hierarchien, mehr Eigenverantwortung und viel Teamarbeit.

In der betrieblichen Praxis führt das dazu, dass Mitarbeiter immer öfter zuhause und unterwegs arbeiten – und sich mit Hilfe moderner Kommunikations- und Kollaborationstools dennoch intensiv austauschen. Aber wie sicher sind die Informationen, die über solche Kanäle versendet werden?

SCHLUSSFOLGERUNG

Damit Vertrauliches vertraulich bleibt, müssen Unternehmen darauf achten, dass die eingesetzten Tools ein Höchstmaß an Datensicherheit garantieren. Das ist gerade auf der Führungsebene wichtig, weil es um besonders sensible Informationen geht – und weil Entscheider ihrer Vorbildfunktion gerecht werden müssen, um auf allen Ebenen des Unternehmens eine IT-Sicherheitskultur zu etablieren.

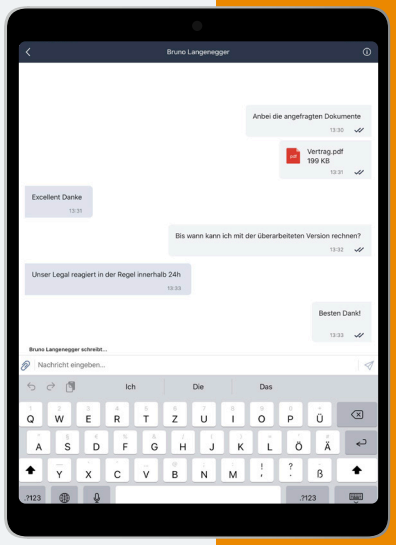
LÖSUNG

Sicherer Datenaustausch leicht gemacht

Mit unserer Software **Diligent Secure File Sharing** (**inkl. Secure Meeting Workflow**) können interne und externe Mitarbeiter Dokumente, die gemeinsam bearbeitet werden sollen, in einer sicheren Umgebung hochladen. Sowohl bei der Übertragung als auch bei der Aufbewahrung sind Informationen vollständig geschützt – dank starker Verschlüsselung, gezielter Zugriffskontrolle und umfassendem Auditing.

Der Austausch von Informationen läuft über ein vollständig privates, Cloud-basiertes Netzwerk, das vom E-Mail-Netzwerk des Unternehmens getrennt und für die **IT-Abteilung nicht sichtbar** ist. Auf diese Weise können Führungsgremien intensiv zusammenarbeiten, ohne Datenklau oder Industriespionage fürchten zu müssen.

Nach unserer Erfahrung ist die E-Mail-Kommunikation eines der größten Einfallstore für Hacker. Mit dem **Diligent Messenger**, der auch als Smartphone- bzw. Tablet-App verfügbar ist, können Gremienmitglieder zudem wesentlich sicherer ad hoc kommunizieren als via E-Mail.



DIE WICHTIGSTEN VORTEILE IM ÜBERBLICK

- Maximale Sicherheit für alle vertraulichen Dokumente
- Effiziente Zusammenarbeit mit internen und externen Parteien
- Dokumentenzugriff von überall und zu jeder Zeit
- Verzicht auf unsichere E-Mail-Kommunikation

HERAUSFORDERUNG DATEN-MANAGEMENT

Wie Unternehmen sichere Daten-Ökosysteme aufbauen – und Industriespione ausbremsen

Die Qualität und Verfügbarkeit von Daten ist ein entscheidender Erfolgsfaktor in der digitalen Ökonomie. Deshalb sammeln immer mehr Unternehmen akribisch Informationen über ihre Kunden und deren Präferenzen.

Auch Echtzeit-Daten aus dem Markt und aus dem eigenen Unternehmen gewinnen rapide an Bedeutung. Schließlich geht es in schnelllebigen Zeiten mehr denn je darum, bei der Unternehmensführung frühzeitig auf Veränderungen reagieren und die richtigen Weichen stellen zu können.

Entscheider brauchen deshalb Daten-Ökosysteme, über die sie schnell und zuverlässig Informationen abrufen können. Das wissen leider auch Cyberkriminelle und Industriespione, die es auf sensible interne Informationen abgesehen haben.

SCHLUSSFOLGERUNG

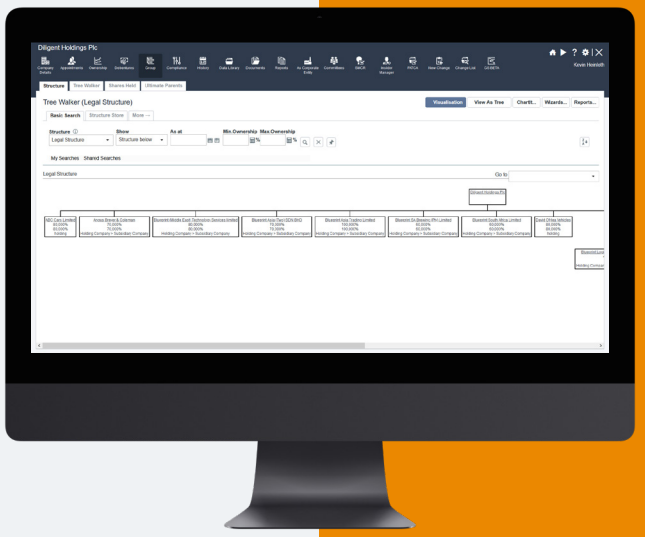
Vorstände und Geschäftsführer müssen dafür sorgen, dass die Datenbanken des Unternehmens bestmöglich vor Unbefugten geschützt sind. Höchste Sicherheitsstandards sind dabei von elementarer Bedeutung, auch in Rechenzentren.

LÖSUNG

Daten und Informationen – zentral und maßgeschneidert

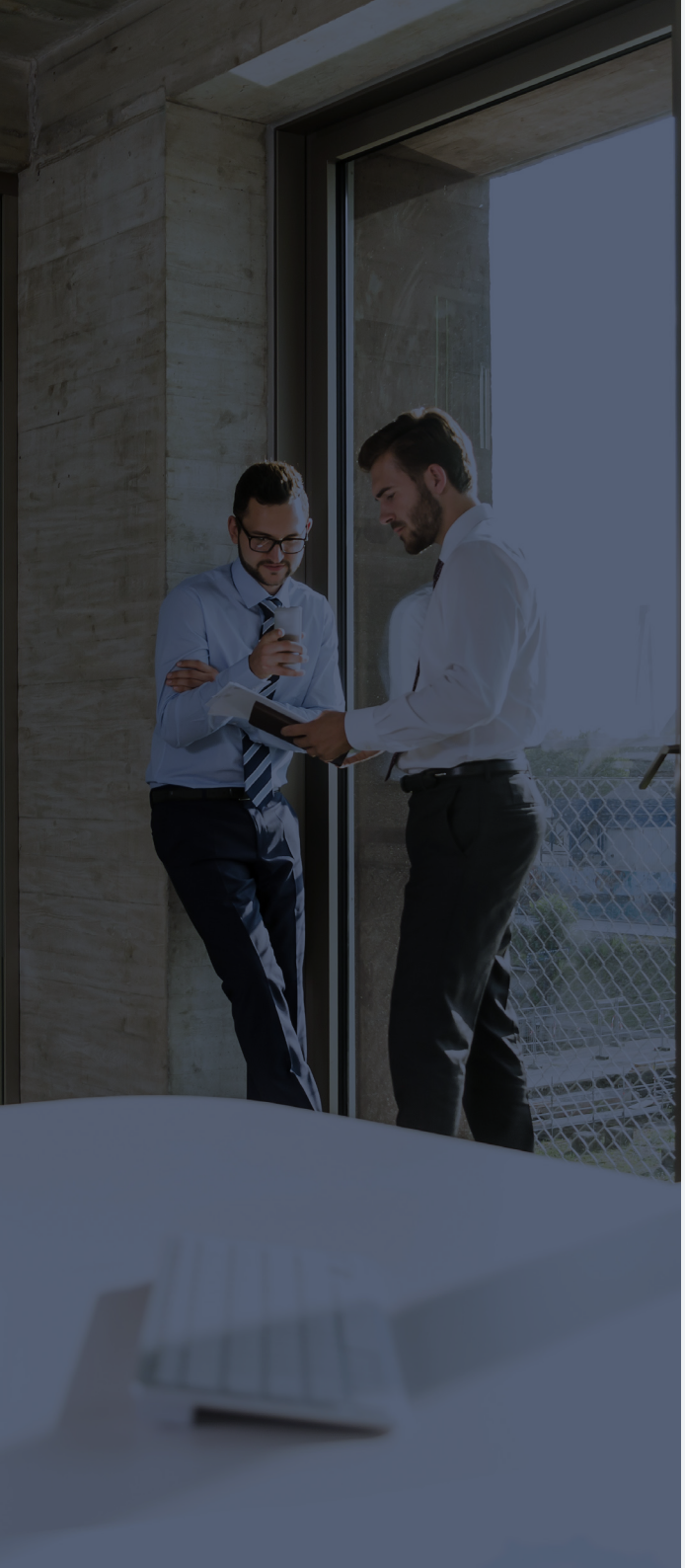
Mit unserer Software **Diligent Entity Management** können Unternehmen interne Daten zentralisieren und verwalten. Sämtliche Informationen, zum Beispiel über Tochtergesellschaften und Beteiligungen weltweit, werden dabei in einem hochsicheren Format gespeichert.

Bei unserer Business-Intelligence-Software **Diligent Governance Intel**, die aus der 24/7-Informationsflut maßgeschneiderte Nachrichten über Ihr Unternehmen, Ihre Wettbewerber und Ihre Branche herausfiltert, ist ebenfalls maximale IT-Sicherheit garantiert. Schließlich soll niemand wissen, was Sie wissen bzw. auf Basis welcher Informationen Sie entscheiden.



DIE WICHTIGSTEN VORTEILE IM ÜBERBLICK

- Informationen zu Beteiligungen zentral und sicher an einem Ort
- maßgeschneiderte Nachrichten zu Unternehmen, Branche und Wettbewerber



HERAUSFORDERUNG DIGITAL-ÖKONOMIE

Wie Entscheider dafür sorgen, dass innovative Angebote benutzerfreundlich und sicher zugleich werden

Kern zukunftsträchtiger Geschäftsmodelle sind oft innovative Online-Portale und Apps. Darüber hinaus entwickeln immer mehr Unternehmen vernetzte Produkte („Internet of Things“) und automatisieren Prozesse und Entscheidungen.

Das zeigt, dass die digitale Transformation ganz verschiedene Bereiche betrifft, in denen sich jeweils unterschiedliche Fragen stellen. Pauschale „one-size-fits-all“-Vorgaben für die Cybersicherheit helfen deshalb oft nicht weiter.

SCHLUSSFOLGERUNG

Entscheider müssen deshalb zunächst sicherstellen, dass die IT-Sicherheit in sämtlichen Bereichen von Anfang an eine zentrale Rolle spielt – und dass die Experten zugleich Spielraum für maßgeschneiderte Lösungen haben. Ein starker Hebel, der im Vergleich zu hohen Compliance-Standards oft unterschätzt wird, ist die Unternehmenskultur.

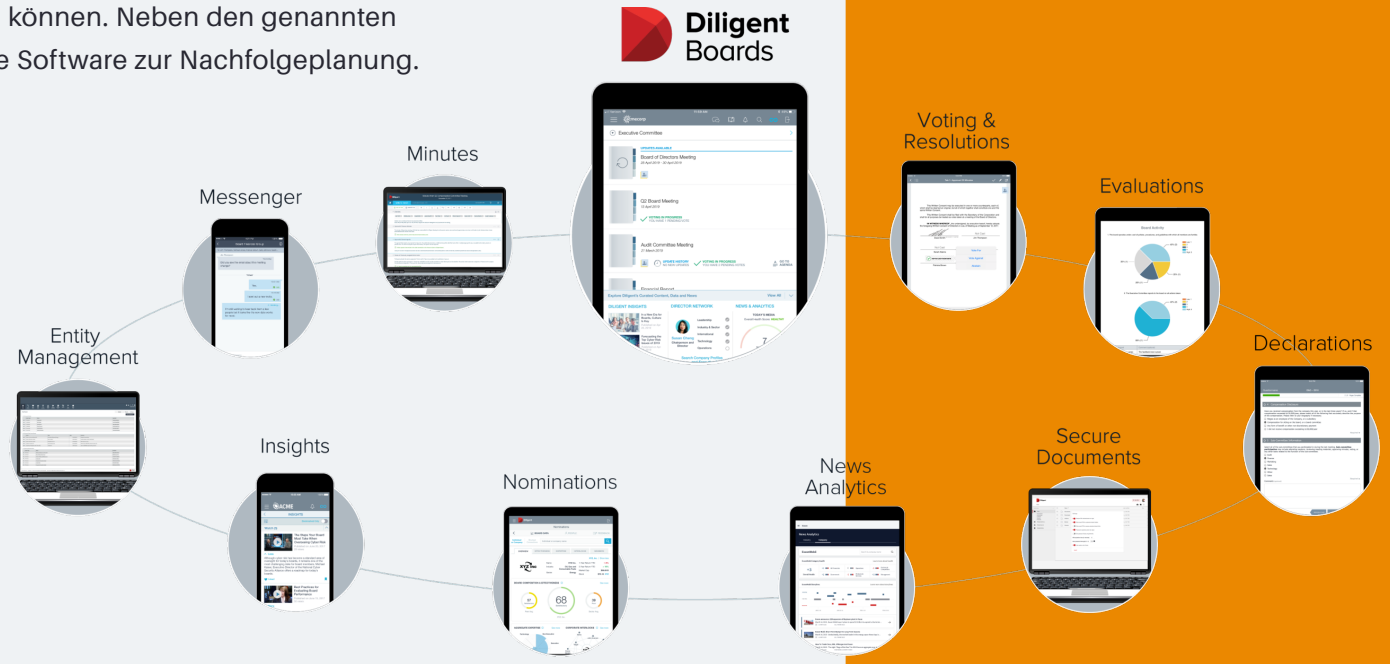
LÖSUNG

Der Aufsichtsrat als Vorbild

Wenn Aufsichtsräte, Vorstände und Geschäftsführer eine **IT-Sicherheitskultur** etablieren wollen, die das gesamte Unternehmen und damit auch die Entwicklung von Online-Portalen, IoT-Produkten und anderen Innovationen prägt, müssen sie mit gutem Beispiel vorangehen (siehe Exkurs „Cybersicherheit & Corporate Governance“ auf der nächsten Seite).

Um sie dabei zu unterstützen, haben wir die **Governance Cloud** entwickelt – als übergreifende Lösung, mit deren Hilfe Entscheider Corporate-Governace-Aufgaben digitalisieren und sicher bewältigen können. Neben den genannten Tools gehört zu dem Paket unter anderem eine Software zur Nachfolgeplanung.

Modern Governance:
Bessere Daten, bessere Fragen, bessere Entscheidungen



EXKURS „CYBERSICHERHEIT & CORPORATE GOVERNANCE“

Überzeugen statt überreden

Wie Aufsichtsräte, Vorstände und Geschäftsführer zu Treibern einer entschlossenen, aber zugleich sicherheitsbewussten digitalen Transformation werden.

Kompetenz. Cybersicherheit beginnt ganz oben. Führungskräfte müssen sich deshalb zwingend mit diesem Thema auskennen. Wer Nachholbedarf hat, sollte nicht zögern, Weiterbildungen zu besuchen sowie interne und externe Experten zu konsultieren. Das gilt auch für Aufsichtsräte. Denn nur, wer über die notwendigen Grundkenntnisse verfügt, kann die richtigen Fragen stellen. Das ist essenziell, um operative Entscheider herauszufordern und Schwachstellen der Unternehmensstrategie bzw. -organisation zu entlarven.

Kultur. Zugleich signalisieren Aufsichtsräte, die sich informieren oder weiterbilden, dass dieses Thema höchste Priorität genießt. Das ist ein wichtiger Schritt, um eine IT-Sicherheitskultur im gesamten Unternehmen zu etablieren – und häufig sogar die Initialzündung. Eine solche Kultur zielt darauf, Mitarbeiter zu überzeugen statt zu überreden und ist damit oft wirkungsvoller als detaillierte Compliance-Kataloge und ausgetüftelte Kontrollmechanismen. Das gilt gerade bei flachen Hierarchien und wachsenden Entscheidungsspielräumen für einzelne Mitarbeiter.

Kommunikation. Wer Menschen überzeugen will, muss den richtigen Ton treffen. Modern Governance heißt deshalb auch: Risiken ansprechen, ohne innovative Ansätze kleinzureden und enthusiastische Mitarbeiter zu entmutigen. Zudem gilt es, mit gutem Beispiel voranzugehen: Aufsichtsräte und Führungskräfte müssen selbst mit digitalen Tools arbeiten, die maximale IT-Sicherheit garantieren – sei es bei der Kommunikation und Kollaboration, bei der Nachfolgeplanung oder beim Herausfiltern wichtiger Nachrichten aus der täglichen Informationsflut.

BRAINLOOP & DILIGENT

Warum wir der richtige Partner für Sie sind

Die Brainloop AG gehört zu den führenden Anbietern Cloud-basierter Lösungen für die vertrauliche Vorstands- und Aufsichtsratskommunikation. Unsere Plattformen sind einfach zu bedienen und nahezu selbsterklärend. Sie ermöglichen Gremienmitgliedern effizientes gemeinsames Arbeiten an Dokumenten und garantieren ein hohes Maß an IT-Sicherheit sowie eine durchgängige Dokumentation. Zu unseren Kunden zählen mittelständische Unternehmen genauso wie internationale Konzerne, darunter mehr als zwei Drittel der DAX-30-Unternehmen.
Weitere Informationen finden Sie auf **www.brainloop.de**.

Seit 2018 gehört Brainloop zur Diligent-Gruppe, dem weltweit führenden Spezialisten für Board-Governance. So vertrauen mehr als 450.000 Mitglieder von Führungsgremien in 14.000 Unternehmen auf das Board-Portal von Diligent – und machen es damit zum meistgenutzten der Welt. Die Daten deutscher und weiterer europäischer Kunden sind ausschließlich auf Servern in Deutschland bzw. der Schweiz und Österreich gespeichert.
Weitere Informationen finden Sie auf **www.diligent.de**.

Hier können Sie unsere Tools testen bzw. einen Demo-Termin vereinbaren

↗ Diligent Secure File Sharing & Secure Meeting Workflow

↗ Diligent Messenger

↗ Diligent Entity Management

↗ Diligent Governance Intel Software

Demo vereinbaren:

↗ https://diligent.com/de/prasentationstermin/

BRAINLOOP Diligent

KONTAKT

Sprechen Sie uns gerne an

Brainloop AG

Mühldorfstrasse 8a
81671 München
Deutschland

T +49 (0) 89 444699 777
E moderngovernance@brainloop.com

Brainloop Austria GmbH

Gonzagagasse 19/3
1010 Wien
Österreich

T +43 (1) 361 99 79 0
E moderngovernance@brainloop.com

Brainloop Switzerland AG

Baarerstrasse 125
6300 Zug
Schweiz

T +41 (0) 44 720 37 37
E moderngovernance@brainloop.com