E-BOOK

So gelingt die DSGVO-konforme Dokumentenreise zwischen Organisationen

Sicherer Dokumentenaustausch für mehr Vertrauen

Vorwort

Reibungsloser Datentransfer zwischen Organisationen

In der digitalen Welt spielt der **sichere** sowie **effiziente Austausch großer Dateien** über Organisationsgrenzen hinweg eine entscheidende Rolle für deren Handlungsfähigkeit und stellt häufig eine Notwendigkeit dar.

Ob es sich um detaillierte Bauzeichnungen, Rechnungen, Pläne, umfangreiche Datensätze oder sensible Dokumentationen handelt – die Fähigkeit, sensible Dateien **DSGVO-konform und einfach zu teilen**, ohne dabei den Prozessablauf einer Organisation und deren Partner zu beeinträchtigen, ist heutzutage unerlässlich.

Dieses Whitepaper beleuchtet die Herausforderungen, Risiken sowie Lösungen für das Teilen umfangreicher Daten und bietet **praktische Empfehlungen für die erfolgreiche Zusammenarbeit** zwischen Organisationen und ihren Partnern. So kommuniziert z. B. der Kreis Borken organisationsübergreifend im Bereich Kinder- und Jugendhilfe und bildet diese effizient ab.

Die Nutzen der Verwaltung lassen sich im Kreis Borken sehen: 150 Rechnungen monatlich, halbjährliche Bewilligungen, Vorlagen und Pläne werden **schnell, transparent und datenschutzkonform** bearbeitet. Das alles unter Einhaltung höchster Standards für die Cybersicherheit.

Pia Lesker
d.velop AG

Gesprächstermin vereinbaren

Im Gespräch erörtern wir, wie Sie einen sicheren, digitalen Dokumentenaustausch in Ihrer Organisation etablieren können.

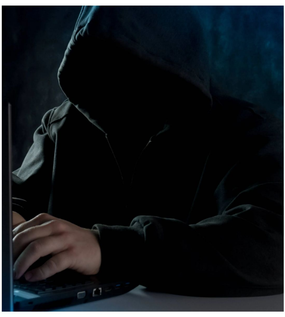
99,2%
Mehr Phishing-Mails im Vergleich zum Vorjahr.

22%
aller Datenschutzverletzungen haben etwas mit Phishing zu tun.

21,2%
aller Deutschen haben schon einmal einen IT-Sicherheitsvorfall erlebt.

Phishing ist die größte Bedrohung für die Cybersicherheit

Das Ziel von Cyberkriminellen ist meist dasselbe: Datendiebstahl. Die Methoden hingegen sind vielfältig: Eine Befragung auf der Online-Plattform statista.de nach den größten Bedrohungen für die Cybersicherheit in den kommenden 12 Monaten ergab, dass das größte Risiko von Phishing (35%), Malware (26%), Datenpannen (25%) und DDoS-Angriffe (21%) ausgehen wird. Aber auch sogenannte Social-Engineering-Angriffe, also die Beeinflussung von meist unbedarften Menschen, um etwa Passwörter zu erbeuten, liegt mit 13 Prozent weit vorn. **Im digitalen Zeitalter sind Daten die Währung schlechthin**. Mit ihnen lässt sich Kasse machen. Und die Schlagzeilen sind gespickt mit Nachrichten über spektakuläre Datendiebstähle.



Daten durchqueren auf ihrer Reise zwischen Organisationen ständig Gefahrenzonen. Eine dieser Gefahren am Wegesrand ist das Phishing – eine betrügerische Technik, die von Cyberkriminellen eingesetzt wird, um **persönliche Informationen wie Benutzernamen, Passwörter, Kreditkarteninformationen und andere sensible Daten und Dokumente** unter Mithilfe ahnungsloser Opfer zu stehlen. Der Begriff „Phishing" leitet sich von der englischen Bezeichnung „fishing" ab, was Angeln bedeutet. Es bezieht sich auf die Taktik, bei der Köder verwendet werden, um Opfer zu täuschen und ihre vertraulichen Informationen preiszugeben.

Daten und Dokumente beim Austausch schützen

Organisationen und Institutionen stehen ständig im Fokus von Kriminellen. Im Jahr 2023 betrugen die Investitionen von Organisationen in Cybersicherheit weltweit rund 80 Milliarden US-Dollar. **Cyberkriminalität richtet finanzielle Schäden durch Erpressungsversuche sowie Geheimnisverrat an und beschädigt dadurch das Vertrauen sowie die Integrität der Organisationen**. Daher ist wichtig, Daten und Dokumente auf ihrer Reise zwischen Organisationen bestmöglich zu schützen, Technik und Mensch vorzubereiten und proaktiv auf Bedrohungen zu reagieren. Denn Phishing-Angriffe variieren in ihrer Raffinesse: von offensichtlich gefälschten E-Mails bis hin zu gezielten Angriffen auf bestimmte Personen oder Organisationen. Die Prävention von Phishing erfordert erhöhte Aufmerksamkeit der Nutzenden, Schulungen zur Erkennung von Phishing-Anzeichen und den Einsatz von Sicherheitsmaßnahmen.

Widerstandsfähigkeit gegenüber Cyberangriffen

Der wichtigste Aspekt im Kontext der Cybersicherheit ist der sichere Austausch von Daten und Dokumenten mit Externen. Die Abwehr von Gefahren und der Schutz der Mitarbeitenden vor riskanten Fehlern haben Priorität. **Die Einführung eines geschützten Raums, in dem Mitarbeitende sicher agieren können, ist entscheidend, um sich vor Cyberangriffen schützen zu können**. Einen solchen geschützten Raum bietet Ihnen d.velop: Einen virtuellen Projektraum, in dem Organisationen DSGVO-konform kollaborieren und sensible Dokumente untereinander und mit ihren Geschäftspartnern sicher austauschen können.

Dokumentenaustausch mit d.velop: idealer Datentransfer für regulierte Märkte

Sichere Räume sind für den Datenaustausch und die Projektarbeit mit Externen bestens geeignet – das gilt vor allem für Organisationen in regulierten Märkten, wie zum Beispiel im Public Sector. In diesem eBook werden wir uns eingehend mit den Möglichkeiten befassen, die d.velop den Organisationen und Institutionen im Cyberraum zur Verfügung stellt. Dabei beleuchten wir auch die Funktionen und Vorteile, die ein gutes Rüstzeug gegen Cyberbedrohungen bieten.

MEHR ZUR LÖSUNG

Mit Ihrem digitalen Whitepaper immer auf dem neuesten Stand

Alle Inhalte in diesem eBook bleiben stets auf dem aktuellen Stand. Über die Pfeil-Symbole am unteren rechten Bildrand können Sie ganz bequem vor und zurück blättern. Außerdem haben Sie die Möglichkeit zwischen den einzelnen Seiten zu wechseln, indem Sie die Kapitel in der oberen Menü-Leiste anklicken.

Sie möchten das eBook als PDF-Dokument erhalten? Kein Problem, das Whitepaper steht Ihnen ebenfalls als Download zur Verfügung. Hier können Sie es herunterladen.

JETZT HERUNTERLADEN

© 2024 d.velop AG

Organisationsübergreifende Vernetzung als Hürde

Wenn Organisationen partnerschaftlich zusammenarbeiten oder in einer Auftraggeber-Dienstleister-Beziehung stehen, nutzen sie oft unterschiedliche Software- und Kommunikationskanäle. Eine der größten Hürden in der organisationsübergreifenden digitalen Vernetzung ist der sichere Austausch von Dokumenten – insbesondere großer Dateien. Organisationen, die sich digital vernetzen möchten, scheitern oft an der Sicherheit. Ihre eigenen Organisationsgrenzen lassen keinen einfachen und sicheren Datenaustausch mit Externen zu. Für Verwaltungen im öffentlichen Dienst **ist es daher oft schwierig, sich miteinander zu vernetzen und Dokumente sicher auszutauschen**.

Technik, Organisation und Regulatorik

Die Gründe für die schwierige Vernetzung finden sich in technischen, organisatorischen und regulatorischen Herausforderungen wider.

So kann der Austausch von Daten…

…über **verschiedene Systeme und Netzwerke** komplex und kostspielig sein.

…eine **enge Zusammenarbeit** zwischen verschiedenen Fachbereichen und Standorten erfordern.

…eine **gemeinsame Sicherheitsstrategie** erfordern.

…durch eine **Vielzahl von Vorschriften und Gesetzen zur Datensicherheit** erschwert werden.

Die Vielzahl unterschiedlicher IT-Systeme

Im öffentlichen Dienst und Hochschul-Bereich gibt es viele Herausforderungen bei der Vernetzung und dem sicheren Austausch von Daten. Partner, Dienstleister, Verbände sowie andere verbundene Organisationen verwenden eine Vielzahl unterschiedlicher IT-Systeme. Die Vernetzung dieser Systeme ist schwierig und kann zu Datenlecks führen.

Voraussetzungen für eine sinnvolle digitale Vernetzung

Doch welche Voraussetzungen müssen erfüllt sein, damit eine digitale Vernetzung möglich und sinnvoll ist? Hier sind zunächst **einige wichtige grundlegende Punkte**, die ausschließlich die Art und Weise der Zusammenarbeit regeln:

Dokumenten-austausch sicher:

Es ist wichtig, Dokumente und größere Dateiformate sicher miteinander teilen und austauschen zu können.

Daten und Informationen:

Organisationen müssen sich darauf einigen, wie sie Informationen austauschen. Das ist wichtig, damit alles reibungslos funktioniert.

Offene Kommunikation:

Alle sollten offen miteinander sprechen. Das hilft, Ideen auszutauschen und voneinander zu lernen.

Gemeinsame Ziele und Strategien:

Alle sollten wissen, wohin die Reise geht. Das bedeutet, dass Organisationen klare Ziele haben und zusammenarbeiten, um diese zu erreichen.

Skalierbarkeit und Flexibilität:

Wenn Projekte wachsen, sollte sich die IT-Infrastruktur in jeder Hinsicht an das Wachstum anpassen können.

Welche Herausforderungen gilt es zu meistern?

In der digitalen Zusammenarbeit mit externen Partnern in regulierten Märkten können verschiedene Hemmnisse auftreten, die die Zusammenarbeit erschweren. Die obige Abbildung zeigt einige davon.

Datenschutz & Compliance

In regulierten Märkten müssen Organisationen strenge Datenschutzbestimmungen und Compliance-Anforderungen einhalten. Der Austausch sensibler Informationen mit externen Partnern oder anderen Organisationen kann zu Datenschutzbedenken und möglichen rechtlichen Problemen führen.

Sicherheitsbedenken

Die Sicherheit sensibler Informationen ist von entscheidender Bedeutung. Bedenken bzgl. der Datensicherheit können dazu führen, dass Organisationen zögern, sensible Daten über digitale Kanäle zu teilen.

Unterschiedliche IT-Systeme & Standards

Partner arbeiten teilweise mit anderen Systemen und Standards. Die Integration kann technische Herausforderungen oder Inkompatibilität mit sich bringen, was den reibungslosen Austausch behindert.

Regulatorische Hürden

Regulatorische Anforderungen können je nach Branche und Region variieren. Unterschiedliche rechtliche Rahmenbedingungen können die Zusammenarbeit beeinträchtigen, da Organisationen sicherstellen müssen, dass ihre digitalen Aktivitäten den geltenden Vorschriften entsprechen.

Mangelndes Vertrauen

Vertrauen ist entscheidend für eine erfolgreiche Zusammenarbeit. Wenn es um den Austausch kritischer Daten geht, fehlt dieses Vertrauen zwischen den Partnern in einigen Fällen möglicherweise.

Komplexität der Prozesse

Die Einführung digitaler Zusammenarbeit erfordert oft Veränderungen in etablierten Prozessen. Diese Umstellungen können komplex sein und bei Mitarbeitenden sowie Externen auf Widerstand stoßen.

Mangelnde Standardisierung

Fehlende Standards für den digitalen Datenaustausch können die Interoperabilität beeinträchtigen. Ohne einheitliche Standards kann ein nahtloser Austausch zwischen verschiedenen Systemen schwierig sein.

Kulturelle Unterschiede

Unterschiedliche Herangehensweisen können die Zusammenarbeit beeinträchtigen. Verschiedene Erwartungen und Arbeitsstile müssen berücksichtigt werden, um Missverständnisse zu vermeiden.

© 2024 d.velop AG

Maßnahmen zur Überwindung von Hemmnissen

Die **digitale Zusammenarbeit mit externen Partnern** ist in vielen Branchen unerlässlich, um Innovationen voranzutreiben, Kosten zu senken und die Zufriedenheit zu steigern. In der öffentlichen Verwaltung ist die digitale Zusammenarbeit jedoch mit besonderen regulatorischen Herausforderungen, wie Datenschutz und Datensicherheit, verbunden. Aber auch die Angst vor Datenmissbrauch bremst die Chancen der Zusammenarbeit über Organisationsgrenzen hinaus stark. Dabei können große und kleine Organisationen sowie Institutionen die digitale Kollaboration mit externen Partnern - und untereinander - durch bestimmte Maßnahmen absichern sowie Hemmnisse minimieren.

Klicken Sie auf die Icons, um eine detaillierte Beschreibungen zu lesen :

1. Erfüllung von Datenschutz- & Compliance-Standards

2. Stärkung der Datensicherheit

3. Standardisierung von Prozessen

4. Klare Kommunikation und Schulung

5. Entwicklung von Partnerschafts-richtlinien

6. Technologische Integration

Diese Maßnahmen zur Hemmnis-Minimierung sind **wichtig, um Kollaboration zu erleichtern und den Austausch von Dokumenten sicher zu gestalten**. Insbesondere die Erfüllung von Datenschutz- und Compliance-Standards ist für Organisationen von entscheidender Bedeutung. Die Europäische **Datenschutz-Grundverordnung (DSGVO) ist ein wichtiger Bestandteil** dieser Standards. Sie **gilt für alle Organisationen und Institutionen, die in der Europäischen Union personenbezogene Daten verarbeiten, wie Hochschulen, Behörden oder Kammern**. Die DSGVO legt strenge Anforderungen an den Datenschutz und die Datensicherheit fest.

Sicherer Datentransfer nach DSGVO

Die **Datenschutz-Grundverordnung (DSGVO)** legt für den sicheren Datentransfer in regulierten Märkten bestimmte Anforderungen fest, wie mit **sensiblen und personenbezogenen Daten im digitalen Umfeld** umzugehen ist. Die folgenden Punkte stellen lediglich einen Überblick dar und sollen nicht als Rechtsberatung verstanden werden. **Es ist wichtig, die spezifischen Anforderungen der DSGVO im Kontext regulierter Märkte und der jeweiligen Branche zu berücksichtigen**:

1. Verschlüsselung:

Die DSGVO verlangt die Verwendung von Verschlüsselungstechnologien, um personenbezogene Daten während des Transfers zu schützen.

2. Integrität der Daten:

Es muss sichergestellt werden, dass die übertragenen Daten während des Transfers unverändert bleiben und vor unbefugten Zugriffen geschützt sind.

3. Zweckbindung:

Personendaten dürfen nur für den festgelegten Zweck übertragen werden, und die Datenübertragung muss für diesen Zweck erforderlich sein.

4. Rechenschaftspflicht:

Verantwortliche müssen nachweisen können, dass sie die Prinzipien der DSGVO einhalten, einschließlich sicherer Datenübertragung.

5. Datenschutz durch Technikgestaltung (Privacy by Design):

Sicherheitsmaßnahmen müssen bereits bei der Konzeption von Datenverarbeitungsprozessen berücksichtigt werden.

6. Meldung von Datenschutzverletzungen:

Im Falle einer Datenschutzverletzung, die zu einem Risiko für die Rechte und Freiheiten von Personen führen könnte, muss die Aufsichtsbehörde unverzüglich informiert werden.

7. Angemessenes Schutzniveau:

Bei der Übermittlung personenbezogener Daten außerhalb der EU muss ein angemessenes Schutzniveau gewährleistet sein, zum Beispiel durch Standardvertragsklauseln oder andere genehmigte Mechanismen.

8. Auftragsverarbeitungsverträge:

Beim Einsatz von Auftragsverarbeitenden muss ein schriftlicher Vertrag abgeschlossen werden, der die Sicherheit und den Schutz der übertragenen Daten regelt.

9. Datensparsamkeit:

Es dürfen nur die für den jeweiligen Zweck notwendigen Daten übertragen werden.

10. Löschungspflicht:

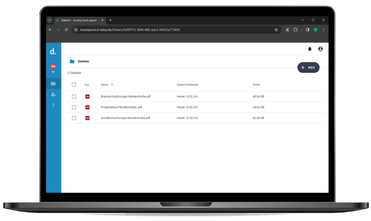
Übertragene Daten dürfen nur so lange aufbewahrt werden, wie es für den festgelegten Zweck erforderlich ist.

© 2024 d.velop AG

Dokumentenaustausch von d.velop: Der sichere Daten-Hafen

Sicheres Arbeiten und Versenden von Dokumenten

Der **sichere Datentransfer zwischen Organisationen** hat enorm an Bedeutung gewonnen. Die Einhaltung der DSGVO ist dabei nicht nur eine rechtliche Verpflichtung, sondern auch entscheidend für das Vertrauen und den **Schutz sensibler Informationen**. In diesem Kontext erweist sich die Lösung der d.velop als **wegweisend** für den Daten- und Dokumentenaustausch. Im Folgenden bieten wir einen detaillierten Einblick in die **Merkmale und Vorteile** unserer Software, die eine sichere sowie effiziente digitale Zusammenarbeit ermöglicht.



Was kann die Lösung?

Diese Lösung von d.velop ist eine fortschrittliche Plattform für den **sicheren Datenaustausch zwischen Organisationen**. Die Lösung ermöglicht es, allgemeine Dokumente, Geschäftsunterlagen und Medien aller Art, **insbesondere aber auch sensible Informationen auf geschützte Weise zu übermitteln und auszutauschen**. Die Software schafft einen digitalen Raum, in dem eine vertrauensvolle Zusammenarbeit möglich ist.

Die Plattform bietet eine sichere Umgebung für den Austausch von Dokumenten und fördert die **organisationsübergreifende Zusammenarbeit in Behörden, Hochschulen oder Kammern**. Durch die Nutzung der d.velop-Lösung können Organisationen sicherstellen, dass ihre digitalen Interaktionen den **höchsten Datenschutzstandards** entsprechen, während sie gleichzeitig sicher, effizient und reibungslos verlaufen.

Hilfreiche Features

DSGVO-konformer Datentransfer:
Gewährleistet einen verschlüsselten und DSGVO-konformen Transfer von Dokumenten und Dateien zwischen Organisationen.

Medienbruchfreie Zusammenarbeit:
Ermöglicht eine nahtlose Zusammenarbeit über Organisationsgrenzen hinweg, ohne Medienbrüche oder Sicherheitsrisiken.

Sicherer Zugriff für Externe:
Externe Partner erhalten einen sicheren Zugriff auf relevante Informationen, was die Zusammenarbeit erleichtert.

Ihre Vorteile

Intuitive Nutzung:
Die Plattform ermöglicht eine eigenständige und einfache Vernetzung mit anderen Organisationen, ohne aufwändige Schulungen oder zusätzliche Software.

Sicherheit & Datenschutz: Entwickelt für höchste Anforderungen in den Bereichen Sicherheit und Datenschutz, um europäische Standards zu erfüllen und Vertrauen zu schaffen.

Verschiedene Medientypen:
Die Plattform unterstützt unterschiedliche Medientypen, darunter Text-, Bild-, Audio- und Videodateien.

Welche Collaborationsfunktionen gibt es?

Die Plattform bietet eine Reihe von medienbruchfreien Funktionen zur digitalen Zusammenarbeit, die es Organisationen ermöglichen, ihre internen und externen Prozesse zu optimieren sowie die **Zusammenarbeit zwischen Mitarbeitenden, Geschäftspartnern und anderen Organisationen zu verbessern**. Es ist eine flexible Plattform, die sich an die individuellen Bedürfnisse von Behörden, Hochschulen oder auch Kammern anpassen lässt. Sie kann in verschiedenen Branchen und für verschiedene Anwendungsbereiche eingesetzt werden. Zu den wichtigsten Funktionen gehören:

Klicken Sie auf die Kästchen, um die Beschreibungen zu lesen →

Collaboration in Spaces

Kommunikation in Spaces

Sicherheit und Datenschutz

WEBINAR

Kooperative Zusammenarbeit mit der eAkte: Plattformübergreifender Dokumentenaustausch im Public Sector

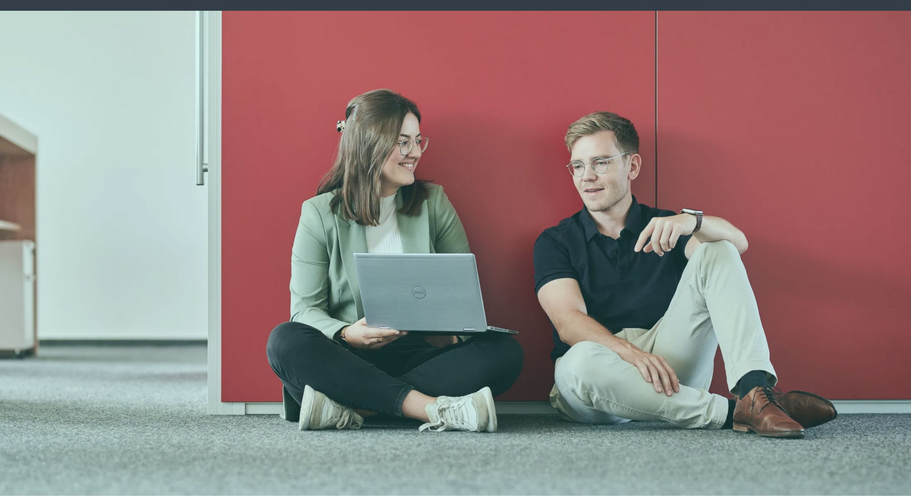
In diesem praxisnahen Webinar erläutern wir den Nutzen der digitalen Zusammenarbeit zwischen Organisationen. Dabei gehen wir auf den DSGVO-konformen, verschlüsselten Transfer der Dokumente und Dateien ein:

- Potenziale der eAkte
- Nutzen digitaler Zusammenarbeit
- Integration in Ihre Prozesse
- Live-Demos digitaler Zusammenarbeit
- Fragen & Antworten

JETZT ANSEHEN

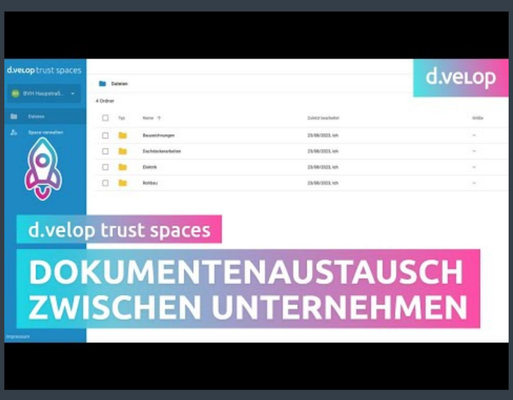
© 2024 d.velop AG

Dokumentenaustausch mit d.velop



So einfach funktioniert der Dokumentenaustausch

Die effiziente Gestaltung von Arbeitsprozessen und die sichere Vernetzung von Organisationen stehen im Mittelpunkt der d.velop-Software. Wie einfach die Plattform funktioniert und welche innovativen Möglichkeiten sie für vernetztes und vertrauensvolles digitales Arbeiten bietet, zeigen wir im Folgenden auf.



Beispiel 1: In Dokumentenräumen grenzenlos zusammenarbeiten

Mithilfe eines einzigen Klicks erstellen Sie einen neuen Space, der mehrere Organisationen miteinander verbindet und vernetztes digitales Arbeiten in einem vertrauensvollen, europäischen Umfeld ermöglicht. Organisieren Sie Ihre Dokumente in Ordnern, teilen Sie sie problemlos über verschiedene Organisationen hinweg, arbeiten Sie gemeinsam an ihnen und erhalten Sie Benachrichtigungen – alles auf unserer benutzerfreundlichen Plattform.

Und das in nur wenigen Schritten:

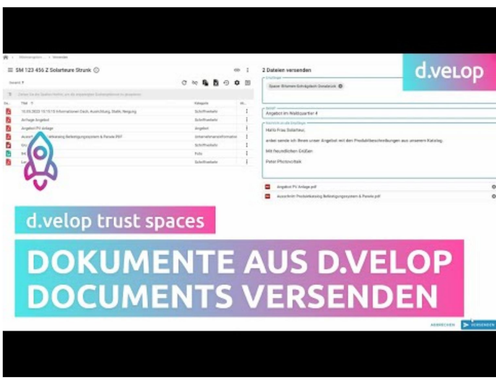
1. Anmeldung auf der Plattform
2. Erstellung & Benennung des neuen Raums
3. Zusammenstellung & Einfügen der Inhalte in den Raum
4. Einladung von Mitgliedern per E-Mail
5. Gemeinsame Bearbeitung der Dateien

Beispiel 2: Wissen aus dem Dokumentenmanagement-Sytem grenzenlos verfügbar machen

Wenn Sie bereits das **DMS d.velop documents** nutzen und Ihr Systemwissen teilen möchten, ist dies problemlos möglich. Übertragen Sie einfach Ihre Dokumente aus d.velop documents in einen gemeinsamen Space mit anderen Organisationen. Wählen Sie die gewünschten Dokumente aus, entscheiden Sie, ob Sie einen bestehenden oder neuen Space verwenden möchten, und übertragen Sie die Dokumente sicher und schnell.

So funktioniert es:

1. Auswahl von Dateien in Akten aus dem DMS
2. Versand der Einladung mit Datei-Zugriff per E-Mail
3. Empfang einer E-Mail mit Betreff und kurzer Zusammenfassung
4. Ansicht des Dokuments auf der Plattform
5. Einfaches Teilen vom Wissen



Highlight

Schnittstelle zum d.velop documents als DMS

- **Wissenstransfer über Organisationsgrenzen hinweg:** Nutzende von d.velop documents können Wissen aus ihrem System einfach in einem gemeinsamen Raum mit anderen Organisationen teilen.
- **Medienbruchfreie Zusammenarbeit:** Dokumente werden sicher und schnell übertragen, was eine effiziente Zusammenarbeit und reibungslose Kommunikation ermöglicht.
- **Rechtssicherheit & Datenschutz:** Die Software erfüllt die Anforderungen an Sicherheit und Datenschutz im Public Sector. Die Plattform ist in Deutschland gehostet und unterliegt den deutschen Datenschutzgesetzen.

Lösung live erleben

Erfahren Sie in einem unverbindlichen Gespräch mit unseren Experten:innen, wie auch Sie einen sicheren, digitalen Datentransfer in Ihrer Organisation erfolgreich etablieren.
Gerne präsentieren wir Ihnen die Software in einer individuellen Live-Demo und beantworten Ihre Fragen.

JETZT TERMIN ANFRAGEN

© 2024 d.velop AG

d.velop-Lösung in der Praxis

d.velop trust spaces

Moderne digitale und sichere Kollaboration zwischen Organisationen und Geschäftspartnern ist mit **d.velop** problemlos möglich. Die Software erleichtert die digitale Zusammenarbeit, gewährleistet einen Datenschutz-konformen Dokumententransfer und bietet innovative Funktionen. Dieser sichere Daten-Hafen ermöglicht es, die Herausforderungen der digitalen Vernetzung zu überwinden und **Dokumente in einer vertrauensvollen Umgebung zwischen verschiedenen Organisationen auszutauschen**. Wie die d.velop-Lösung von der öffentlichen Verwaltung innerhalb verschiedener Anwendungsbereiche genutzt wird, lesen Sie hier.

Kinder- und Jugendhilfe

In der Kinder- und Jugendhilfe kooperieren Jugendämter und freie Träger gemäß SGB VIII, um Schulbegleitungen für junge Menschen oder Familien zu organisieren. Gemeinsame Hilfeplangespräche werden protokolliert. Monatliche Rechnungen werden zwischen Träger und Jugendamt abgestimmt. Die Funktion "Konversation mit Dokumenten" erleichtert die Rechnungsstellung.

Bauamt

Bei Bauprojekten müssen Dokumente wie Brandschutz- oder Schallschutzkonzepte mit Partnerunternehmen geteilt werden. Hierfür bietet sich die Nutzung von "Teamspaces" an. Das Bauunternehmen legt Projektdokumente in gemeinsamen Teamspaces mit Subunternehmen ab.

Rechnungsverarbeitung

Das Gebäudemanagement einer Stadt nutzt externe Ingenieur- und Architektenbüros für die Verwaltung verschiedener Immobilien. Diese prüfen Rechnungen vor der Weiterverarbeitung durch die Stadt. Der "Verfügungsworkflow" der d.velop unterstützt diesen Prozess, inklusive der Funktion "Konversation mit Dokumenten" für die Bereitstellung von Prüfungsunterlagen.

Sie haben einen weiteren Anwendungsfall?

Kontaktieren Sie uns und wir besprechen Ihre individuellen Anforderungen!

Die sichere Datenreise zwischen Organisationen ist eine der Kernherausforderungen im digitalen Zeitalter. Insbesondere hinsichtlich des Phishings, der wohl bedeutendsten Bedrohung für die Cybersicherheit, sind Maßnahmen zur sicheren Kollaboration und zum sicheren Dokumentenaustausch unabdingbar. Die Einführung von geschützten Räumen bietet einen sicheren virtuellen Projektraum für den DSGVO-konformen Dokumentenaustausch.

JETZT ANSPRECHEN

© 2024 d.velop AG

Die d.velop AG

Die d.velop AG hilft Ihren Kunden:innen durch den Einsatz der Software für Dokumentenmanagement und digitale Geschäftsprozesse dabei, ihr ganzes Potenzial zu entfalten. Ganz konkret, indem die d.velop AG digitale Dienste bereitstellt, welche die Menschen miteinander verbinden, sowie Abläufe und Vorgänge umfassend vereinfachen und neu gestalten.

Über d.velop

Die d.velop-Gruppe mit Hauptsitz in Gescher entwickelt und vermarktet Software zur durchgängigen Digitalisierung von Geschäftsprozessen und branchenspezifischen Fachverfahren und berät Unternehmen gemeinsam mit einem Netzwerk aus Hunderten Partnern in allen Fragen der Digitalisierung. Mit der Ausweitung des etablierten Content Services / ECM-Portfolios rund um Dokumentenmanagement, digitale Archivierung und Collaboration bietet der Software-Hersteller die Software in allen Bereitstellungsformen als SaaS, on Premises und Hybrid an. Dank HTML5-Technologie sind diese Produkte auf beliebigen Endgeräten nutzbar. Dabei werden die Rechtssicherheit und die Einhaltung gesetzlicher Vorgaben dank eines ausgereiften Compliance Managements optimal unterstützt.

d.velop stellt digitale Dienste bereit, die Menschen miteinander verbinden, sowie Abläufe und Vorgänge umfassend vereinfachen und neugestalten. So hilft der CSP- / ECM-Spezialist Unternehmen und Organisationen dabei, ihr ganzes Potenzial zu entfalten.

Ein starkes, international agierendes Netzwerk aus **rund 400 spezialisierten Partnern** macht d.velop Produkte weltweit verfügbar.

d.velop-Produkte sind branchenübergreifend bislang bei **mehr als 13.000 Kunden mit über 3,2 Millionen Anwendern** im Einsatz, darunter Tupperware Deutschland, eismann Tiefkühl-Heimservice GmbH, Parker Hannifin, Nobilia, Schmitz Cargobull, FingerHaus GmbH, die Stadt Wuppertal, die DAK-Gesundheit, DZ Bank AG, das Universitätsklinikum des Saarlands oder die Diakonische Einrichtungen in Hessen und Nassau GmbH.

HIER GEHT'S ZUR INDIVIDUELLEN LIVE DEMO

d.velop AG
Schildarpstraße 6-8
48712 Gescher
Deutschland

Kontakt
+49 2542 9307-0
d-velop.de

Handelsregister Coesfeld: HRB 4903;
USt-IdNr. DE 813062165

Impressum | Datenschutz

Vorstand der d.velop AG
Rainer Hehmann
Dr. Stephan Held
Christoph Pliete

Aufsichtsratsvorsitzender
Dr. Helmut Bäumer

1. Erfüllung von Datenschutz- & Compliance-Standards

Implementierung von Technologien und Prozessen, die den Datenschutz und die Einhaltung von Vorschriften gewährleisten.

Schließen

5. Entwicklung von Partnerschafts-richtlinien

Erstellung klarer Partnerschaftsrichtlinien, die Datenschutz, Sicherheit und Prozessstandards für alle Parteien festlegen.

Schließen

2. Stärkung der Datensicherheit

Investitionen in Sicherheitslösungen und die Implementierung bewährter Sicherheitspraktiken, um Bedenken hinsichtlich der Datensicherheit zu adressieren.

Schließen

3. Standardisierung von Prozessen

Vereinheitlichung von Prozessen und die Einführung gemeinsamer Standards, um die Komplexität zu reduzieren und die Interoperabilität zu verbessern.

Schließen

6. Technologische Integration

Investition in Technologien, die eine nahtlose Integration unterschiedlicher IT-Systeme ermöglichen, um Inkompatibilitäten zu überwinden.

Schließen

4. Klare Kommunikation & Schulung

Kommunikation der Vorteile der digitalen Zusammenarbeit und Schulung aller beteiligten Parteien, um Vertrauen aufzubauen und Widerstände zu minimieren.

Schließen

Kommunikation in Spaces

Die Software bietet verschiedene Kommunikationsfunktionen, darunter einen Chat. Diese Funktionen ermöglichen es den Nutzenden, sich in Echtzeit auszutauschen und zusammenzuarbeiten.

Schließen

Collaboration in Spaces

Die Software-Lösung ermöglicht die **Zusammenarbeit in virtuellen Räumen**, sogenannten Spaces. In einem Space können Nutzende Dokumente, Dateien, Links und andere Inhalte gemeinsam speichern, bearbeiten und diskutieren.

- Erstellen und Verwalten von Spaces
- Hinzufügen und Entfernen von Mitgliedern
- Teilen von Dokumenten, Dateien, Links und anderen Inhalten
- Kommentieren und diskutieren von Inhalten
- Vertrag mit Schriftformerfordernis = Qualifizierte elektronische Signatur

Schließen

Sicherheit und Datenschutz

Die Software erfüllt die hohen Anforderungen an **Sicherheit und Datenschutz** in regulierten Märkten wie dem Public Sector. Davon profitieren auch die Geschäftspartner. Die Plattform ist in Deutschland gehostet und unterliegt den deutschen Datenschutzgesetzen.

- Verschlüsselung von Daten
- Zugriffskontrolle

Schließen

epcan GmbH

Branche: Internet
Anwendungsfall: digitalisierung von Auftragsvormularen über die d.velop sign API

"Früher haben wir Anträge und Befragungen mit Papier gemacht, per Post. Ein Riesenprozess. Aufwändig und unnötig. Zunächst sind wir bei Docusign gelandet. Das war für uns aber nicht mehr als eine Eingabeerleichterung. Damit waren wir noch nicht am Ziel. d.velop sign generiert für uns einen digitalen Vertrag, den unser potenzieller Kunde in Echtzeit bekommt. Alles ist vollständig integriert, alle Daten sind digital, kein Mitarbeiter muss mehr diese Buchung anfassen. Das ist für uns natürlich perfekt."

Nils Waning
Geschäftsführender Gesellschafter
epcan GmbH

ZURÜCK

Energiekontor AG

Branche: Windkraft
Anwendungsfall: Jahresabschlüsse digital unterschreiben

"Früher haben wir die Dokumente ausgedruckt und diese zur Unterschrift in den Umlauf zu den Geschäftsführern gegeben. Mit der Coronakrise ist die digitale Unterschrift unverzichtbar geworden, da das Unterzeichnen auf Papier, nicht zuletzt auch durch den Einsatz von Kurieren sehr aufwendig und zeitfressend war. d.velop sign ist für uns alle eine extreme Arbeitserleichterung. Wir sparen uns Tausende Blatt Papier pro Jahr, viele Arbeitsstunden und erhebliche Kosten."

Jacqueline Afzali
Verwaltungs-Mitarbeiterin
Energiekontor AG

ZURÜCK

Filmakademie Baden-Württemberg

Branche: Film
Anwendungsfall: Arbeitsverträge digital unterschreiben

"Zu Spitzenzeiten haben wir im Monat 200 Verträge gedruckt, unterschrieben und verschickt. Wir haben keine eigenen Lehrenden, sondern arbeiten nur mit Gast-Lehrenden, aus der ganzen Welt. Bei über 550 externen Lehrenden pro Jahr und bis zu fünf Verträgen pro Lehrenden kommt da schon viel Papier zustande. Und viel Arbeit, ich selbst leiste am Tag manchmal 100 Unterschriften. Mit d.velop sign sparen wir uns das Ausdrucken und das Unterzeichnen per Hand. Der Zeitgewinn ist immens."

Günter Herwig
Leitung Personal und Honorare
Filmakademie Baden-Württemberg GmbH

ZURÜCK

Warth & Klein Grant Thornton AG

Branche: Wirtschaftsprüfung
Anwendungsfall: Prüfungsberichte digital unterschreiben

"Früher haben wir rund 30.000 Prüfungsberichte im Jahr gedruckt, mit insgesamt bis zu drei Millionen Seiten. Darunter bis zu 120.000 Unterschriften. Das Erstellen und die Freigabe der Berichte lief noch elektronisch, dann kam der Prozessbruch – die Unterschrift. Heute sind wir mitten in der Umsetzung, einen Großteil der bis zu 3500 Prüfungen jährlich intern elektronisch zu signieren. Einige hundert funktionieren schon mit d.velop sign, und es werden immer mehr. Allein der Bereich Logistik rund um die Prüfungsberichte ist so auf einen Bruchteil geschrumpft. Es ist ein großer Effizienzgewinn."

Philipp Wiesauer
Leiter Strategische Digitalprojekte
Warth & Klein Grant Thornton AG

ZURÜCK

Lohmann & Rauscher GmbH & Co. KG

Branche: Medizinfabrikant
Anwendungsfall: Schulungsunterlagen digital unterschreiben

"Früher haben wir viele Dokumente, die unterzeichnet werden mussten, ausgedruckt und in die Hauspost gegeben. Eine Assistentin hat dann die Post ausgepackt, die entsprechenden Dokumente hingelegt und nach der Unterschrift wieder eingepackt und zurückgeschickt. Wenn das 3000 Mitarbeiter regelmäßig machen, und dann auch noch zwischen Standorten in Deutschland und Österreich, dann ist das nicht nur viel Papier, sondern auch viel Rennerei.“

Maximilian Rumpf
IT-Consultant für Corporate Functions
Lohmann & Rauscher

ZURÜCK

PKF WMS

Branche: Beratungsgesellschaft
Anwendungsfall: Prüfungsberichte digital unterschreiben

"Wenn ein finaler, unterschriebener Bericht ausgeliefert werden sollte, konnte es vorkommen, dass wir da schon beim nächsten Mandanten waren“, beschreibt. Vor d.velop sign mussten Mitarbeiter manchmal einen Umweg über das Büro machen, nur um eine Unterschrift zu leisten. Dabei haben wir Tage verloren. Wir wollten vom Papier weg und effizienter, ökologischer und flexibler arbeiten.“

Michael Strack
Abteilungsleiter für den Bereich Wirtschaftsprüfung
PKF WMS

ZURÜCK

Einfache elektronische Signatur

Die einfache elektronische Signatur besteht aus Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet (Art. 3 Nr. 10 eIDAS-VO). Es genügt daher, dass für den Empfänger des elektronischen Dokuments die Person des Erklärenden erkennbar ist. Diese Zuordnungs- und Identitätsfunktion von elektronischen Signaturen liegt beispielsweise in den folgenden Fällen vor:

- eingescannte und im Dokument eingefügten Unterschrift
- unter einer E-Mail eingetippte Unterschrift
- durch Programm automatisch eingefügte E-Mail-Signatur

ZURÜCK

Fortgeschrittene elektronische Signatur

Die fortgeschrittene elektronische Signatur beinhaltet zusätzliche Voraussetzungen, um die leichte Manipulierbarkeit der „einfachen“ elektronischen Signaturen zu verhindern (Art. 3 Nr. 11 i. V. m. Art. 26 eIDAS-VO). Eine fortgeschrittene elektronische Signatur muss kumulativ folgende Anforderungen erfüllen:

- sie ist eindeutig dem Unterzeichner zugeordnet;
- sie ermöglicht die Identifizierung des Unterzeichners;
- sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann;
- sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

ZURÜCK

Qualifizierte elektronische Signatur

Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur gem. Art. 26 eIDAS-VO, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat eines qualifizierten Vertrauensdiensteanbieters für elektronische Signaturen beruht (Art. 3 Nr. 12 eIDAS-VO). Sie muss kumulativ folgende Voraussetzungen erfüllen:

- sie erfüllt alle Voraussetzungen einer fortgeschrittenen elektronischen Signatur
- sie muss von einer qualifizierten elektronischen Sicherstellungseinheit erstellt werden
- sie muss auf einem qualifizierten Zertifikat beruhen

ZURÜCK

Die eIDAS-Verordnung auf einen Blick

- **Name:** eIDAS (Abkürzung für: electronic IdDentification, Authentication and trust Services)
- **Verordnung:** EU-Verordnung 910/2014
- **Titel:** Verordnung des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
- **Inhalte:** elektronische Signaturen (eIDAS-Signaturen), Siegel, Zeitstempel und Einschreiben sowie Webseiten-Zertifikate
- **Geltungsbereich:** europaweit (EU-Mitgliedsstaaten und Europäischer Wirtschaftsraum)
- **Inkrafttreten:** 17. September 2014
- **Anzuwenden:** 01. Juli 2016

ZURÜCK

Digital unterschreiben in Microsoft Teams

Microsoft Teams ist mit 250 Millionen monatlichen Usern eine der meistgenutzten Apps der Welt und für viele besonders durch das vermehrte Arbeiten im Home-Office nicht mehr wegzudenken. Auch haben digitale Unterschriften in den letzten Monaten einen gewaltigen Boost erfahren, da sie nie notwendiger waren als heute.

Durch eine brandneue Schnittstelle von CONTENiT ist es nun möglich, dass Dokumente direkt in Microsoft Teams nahtlos digital unterschrieben werden können. Dieses besondere Zusammenspiel ist ein absoluter Game-Changer und macht sowohl Ihre tägliche Teams-Kommunikation als auch Ihre Prozesse schneller und effizienter.

Zum Webinar

Dokumente in Microsoft 365 digital signieren

Ist Microsoft 365 als zentrale Plattform im Unternehmen integriert, so besteht nicht nur die Notwendigkeit den bis dato fehlenden digitalen Ende-zu-Ende Prozess mit den konkreten Anforderungen der Unternehmen an eine Rechtsverbindlichkeit der Signaturen (Anforderungen der EU nach eIDAS-Verordnung) zu bedienen, sondern auch eine native Verfügbarkeit für den SharePoint zu gewährleisten.

Ganzen Artikel lesen

Welches Signaturlevel kommt wann zum Einsatz?

Bescheinigung = Einfache elektronische Signatur
Jahresabschluss = Qualifizierte elektronische Signatur
Datenübermittlung = Einfache elektronische Signatur
Vertrag ohne Schriftformerfordernis = Einfache elektronische Signatur
Vertrag mit Schriftformerfordernis = Qualifizierte elektronische Signatur
SEPA Mandat = Einfache elektronische Signatur

ZURÜCK

Welches Signaturlevel kommt wann zum Einsatz?

- Bescheinigung = Einfache elektronische Signatur
- Jahresabschluss = Qualifizierte elektronische Signatur
- Datenübermittlung = Einfache elektronische Signatur
- Vertrag ohne Schriftformerfordernis = Einfache elektronische Signatur
- Vertrag mit Schriftformerfordernis = Qualifizierte elektronische Signatur
- SEPA Mandat = Einfache elektronische Signatur

Close

1. Datendiebstahl und Verlust von Vertraulichkeit

- Phishing-Angriffe zielen oft darauf ab, Informationen wie **vertrauliche Dokumente, Finanz- oder Personen-Daten** zu stehlen. Deshalb sind diese in besonderem Maße auf einen sicheren, vertrauensvollen Dokumentenaustausch zwischen Organisationen angewiesen.

- Gelingt Kriminellen doch ein erfolgreicher Diebstahl, **kann** der Verlust von Geschäftsgeheimnissen **erhebliche finanzielle Verluste nach sich ziehen**.

Schließen

2. Identitätsdiebstahl und Betrug

- Datendiebe können gestohlene Zugangsdaten dazu verwenden, sich als legitimer Benutzer auszugeben und **betrügerische Aktivitäten im Namen der Organisation** durchzuführen.

- Organisationen und ihre Mitarbeitenden könnten Opfer von Betrug werden, wenn Angreifende Zugang zu internen Systemen und Finanzinformationen erhalten.

Schließen

3. Reputationsschaden

- Ein erfolgreicher Phishing-Angriff hat das Potenzial, das Ansehen und den Ruf einer Organisation erheblich zu beeinträchtigen. Wenn beispielsweise Informationen über Bürger:innen, Geschäftspartner oder Studierende durch ein Datenleck an die Öffentlichkeit gelangen, verlieren diese Vertrauen in die Sicherheitsmaßnahmen der Verwaltungsorganisation, was **langfristige Auswirkungen auf die Geschäftsbeziehungen** haben kann.

Schließen

4. Unterbrechung der Handlungsfähigkeit

- Phishing-Angriffe können Geschäftsunterbrechungen nach sich ziehen, um geheime Dokumente zu sichern. Das ist insbesondere dann der Fall, wenn **Ransomware oder andere schädliche Software** in die internen Systeme gelangt ist.

- Die Säuberung und Wiederherstellung der IT-Systeme nach einem Angriff erfordern **nicht nur erhebliche Ressourcen, sondern ziehen ersichtliche Ausfallzeiten** nach sich, was sich negativ auf die Produktivität und Services auswirkt.

Schließen

5. Compliance-Verletzungen

- Organisationen in regulierten Märkten sind gesetzlich dazu verpflichtet, strenge Datenschutzstandards einzuhalten. Das betrifft insbesondere die Speicherung und den Austausch von Dokumenten mit persönlichen und schützenswerten Informationen. **Erfolgreiches Phishing stellt eine Compliance-Verletzung dar, die rechtliche Konsequenzen nach sich ziehen kann**.

Schließen

6. Kosten für Sicherheits-maßnahmen & Schulungen

- Damit sich Organisationen und Institutionen vor Phishing-Angriffen schützen und am Ende ihre vertraulichen Daten geheim halten können, müssen sie **ausreichend Ressourcen** für Sicherheitsmaßnahmen wie Firewalls, Anti-Phishing-Tools und Schulungen für Mitarbeitende investieren.

Schließen

7. Vertrauensverlust

- Bürger:innen oder Studierende, die sich unsicher bezüglich der Sicherheit ihrer Daten fühlen, neigen dazu, das Vertrauen in die jeweilige Organisation zu verlieren. Skepsis gegenüber der Verwaltungsorganisation kann **nachhaltig negative Auswirkungen** zur Folge haben.

Schließen