Immer sicher
mit Fellow Digitals

fellow digitals

Succeeding together

Inhalt

Sicherheit in guten Händen
mit Fellow Digitals

Im Zeitalter der DSGVO ist die Datensicherheit essentiell. Unsere Kunden vertrauen darauf, dass die Sicherheit ihrer Daten und Informationen für uns immer oberste Priorität hat. In diesem Whitepaper können Sie lesen, wie Fellow Digitals die höchstmöglichen Sicherheitsstandards erfüllt. So ermöglichen wir allen, jederzeit sicher zu arbeiten, egal wo sie sich befinden.

Bei Sicherheit gehen wir keine Kompromisse ein. Seit 1997 vertrauen unsere Kunden darauf, in einer sicheren und zuverlässigen Umgebung arbeiten zu können. Auch bei der Anbindung oder Integration anderer Plattformen oder bei der Einladung externer Nutzer. Unsere Server werden 24 Stunden am Tag von einem niederländischen Hosting-Provider überwacht, im Wissen, dass die Sicherheit aller unbeeinträchtigt bleibt.

ISO 27001 ist eine international anerkannte Sicherheitsnorm, die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung von Managementsystemen für Informationssicherheit festlegt. Es ist wichtig zu wissen, dass Fellow Digitals zusätzlich dazu über das NEN 7510-Zertifikat verfügt, das sich auf die Informationssicherheit im Gesundheitswesen konzentriert.

Seit 2022 ist Fellow Digitals auch nach ISO 27701 zertifiziert. Die internationale Norm ISO 27701 enthält Richtlinien zum Datenschutz, zum Umgang mit personenbezogenen Daten in Unternehmen und zur weltweiten Einhaltung von Datenschutzbestimmungen.

Sicherheit, **Compliance** und **Zertifizierung**

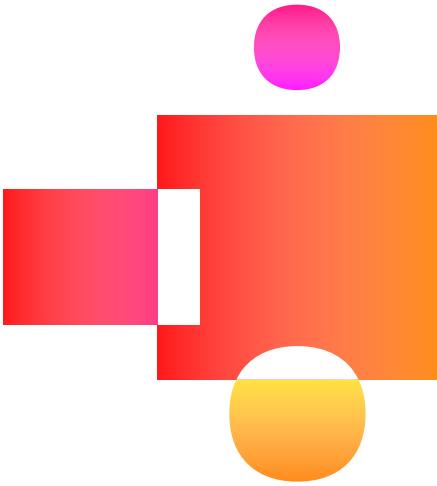
Bei Fellow Digitals steht die Sicherheit Ihrer Unternehmensdaten immer an erster Stelle. Unsere Server werden in den Niederlanden gehostet und rund um die Uhr überwacht. Wir halten uns an die EU-Datenschutz-Grundverordnung (DSGVO). Diese Verpflichtung wird durch unsere Zertifizierungen nach ISO/IEC 27001, ISO/IEC 27701 und NEN 7510 untermauert.

Datenschutz-Grundverordnung

Die Produkte von Fellow Digitals werden in den Niederlanden gehostet. Unsere Sicherheitsstandards erfüllen die Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO) und gelten für Mitarbeiter-, Stakeholder- und Kundendaten.

Wir verbessern unsere Sicherheitsmaßnahmen kontinuierlich. Im Jahr 2022 haben wir die Zertifizierung nach ISO/IEC 27701 erhalten, einer Erweiterung der ISO/IEC 27001, die sich auf die Verwaltung und den Schutz personenbezogener Daten konzentriert.

Unsere Mitarbeiter werden regelmäßig zu den aktuellen Datenschutzbestimmungen geschult, sodass sie über aktuelles Wissen verfügen, um Ihre Daten zu schützen.



Zertifikate Fellow Digitals

ISO 27001

Fellow Digitals ist nach ISO 27001 zertifiziert. Das bedeutet, dass wir die höchsten Anforderungen an die Daten- und Informationssicherheit erfüllen. Nutzer können die Produkte von Fellow Digitals ohne Sicherheitsbedenken nutzen. Mit dem ISO 27001-Zertifikat legt Fellow Digitals Folgendes vor:

- Sorgfältiger Umgang mit Daten auf allen Ebenen
- Einhaltung von Gesetzen und Vorschriften
- Ein glaubwürdiges und professionelles Unternehmen zu sein
- Verringerung der Möglichkeit von Risiken und Zwischenfällen

ISO 27701

ISO 27701 ist eine Erweiterung der ISO-Norm 27001 für Informationssicherheit. Sie enthält spezifische Leitlinien für den Schutz der Privatsphäre und Verwaltungsmaßnahmen für datenschutzrelevante Daten.

Dieser Standard bietet die Gewissheit, dass Fellow Digitals die internationalen Anforderungen an den Schutz personenbezogener Daten im weitesten Sinne des Wortes erfüllt.

NEN 7510

Wo sich die ISO 27001 Zertifizierung auf “allgemeine” Daten- und Informationssicherheit konzentriert, befasst sich die NEN 7510 Zertifizierung speziell mit dem Schutz von Gesundheitsdaten. Das Qualitätszeichen NEN 7510 ist ein höchst relevantes Zertifikat für verschiedene Kunden von Fellow Digitals, vor allem im Gesundheitssektor.

Sicherheit von
Hosting- und Datenzentren

Persönliche Daten, Dokumente und Firmeninformationen. Dies sind nur einige Beispiele für Daten, die in den Fellow Digitals Plattformen eingestellt und verwaltet werden können. Diese Daten werden an einem physischen Ort gespeichert, der den höchstmöglichen Sicherheitsanforderungen entspricht. Dadurch wird das Risiko von Zwischenfällen oder Diebstahl auf ein Minimum reduziert.

Die Server von Fellow Digitals werden von Exonet gehostet und verwaltet. Exonet ist nach ISO 27001, ISO 9001 und NEN 7510 zertifiziert und erfüllt somit die höchsten Sicherheitsstandards. Unsere Server befinden sich in Rechenzentren von BIT in Ede (Niederlande). Backups werden in einem zweiten Rechenzentrum gesichert: Smartdc in Rotterdam.

Unsere Server sind standardmäßig mit den neuesten Sicherheits-Patches ausgestattet. Die Server befinden sich hinter einer Firewall, wodurch sie für Hacker und andere Eindringlinge unzugänglich sind.

Merkmale von Exonet (Managed Hosting)

- ISO 27001, ISO 9001, und NEN 7510 zertifiziertes verwaltetes Hosting
- Kundenorientierung und -zufrieden heit, Beschwerdemanagement
- Serviceprozesse, Produktentwicklung
- Qualitätsprüfungen
- Integration von Produkten und offenen Standards
- Service Level Agreement (SLA)
- Uptime von min. 99,9%
- Hosting und Wartung der Systeme
- Testsysteme, -verfahren und -vorfälle

Merkmale von BIT und Smartdc (Datenzentren)

- ISO 27001
- NEN 7510
- Ausweichstandort

Ausweichstandort

Wir wollen nicht schwarzmalen, aber was, wenn einer oder mehrere Server aufgrund einer Katastrophe ausfallen? Bei Fellow Digitals gehen wir kein Risiko ein. Aus diesem Grund werden wir ab 2021 einen Ausweichstandort haben. Dabei handelt es sich um eine Serverumgebung, die mit der Umgebung in unserem Hauptrechenzentrum identisch ist und ebenfalls von unserem Hosting-Provider Exonet verwaltet wird. Auf diese Weise können Sie blitzschnell auf Ihre Daten zugreifen.

Physischer Server-Schutz

- 24/7 Besetzung des Operationszentrums
- 24/7 Sicherheitspatrouillen
- Ständige Sicherheit durch Überwachungskameras
- Sicherheit vor unbefugtem Zutritt und Alarmschutz auf dem Gelände und im Gebäude
- Zugang zum Gebäude und zum Gelände nur über Sicherheitsschlösser und Absperrungen
- VEB-zertifizierte Schutzklasse 4
- Alternativer Wiederherstellungsort

Verwaltung kritischer Umgebungen

- Erfahrenes Managementteam
- (Thermische) Klimatisierung
- Kontinuierliche Überwachung von Gebäudeleittechnik (GLT)
- International anerkanntes Critical Environment Program

Stromversorgung

- Stromversorgung: 50 kV
- Unterbrechungsfreie Stromversorgung – bis zu 48 Stunden bei voller Kapazität
- 1.500 W/m2 (Erhöhung möglich)

Patch-Verwaltung

Sicherheitsupdates und Betriebssystem-Patches werden täglich installiert. Dringende Hotfixes werden auf Anfrage durchgeführt (Notfallwartung). Für jede Version von Fellow Intranet oder Fellow LMS werden die Code-Abhängigkeiten aktualisiert. Zur Überprüfung des Patch-Verwaltungsprozesses führt eine Drittpartei (in diesem Fall Securify) regelmäßige Überprüfungen durch. Mehr dazu können Sie im Abschnitt “Externe Prüfungen” lesen.

Digitaler Schutz

- SSL/HTTPS-Verschlüsselung
- Firewalls
- Regelmäßige Sicherheits-Patches
- Penetrationstests
- 24/7 Server-Überwachung
- Verwaltung über separates VPN-Netzwerk
- Server-Virtualisierung
- Zentrale Protokollierung
- Off-Site-Sicherung
- Ecrypted Data Storage

Gebäude und Brandschutz

- Rauch- und Feuermelder im gesamten Gebäude
- Inergen-Gas (Feuerlöscher) in technischen Abteilungen
- Wände und Dach aus Beton

Serverstandort im Rechenzentrum

- Hardware in kundenspezifischen Gestellen im lokalen Rechenzentrum in Ede (NL)
- Virtuelle Hardware für erhöhte Verfügbarkeit und Skalierbarkeit
- Hardware vervielfältigt

Sicher durch Design
Software-Entwicklung

Fellow Digitals entwickelt seine Software nach dem Prinzip “sicher durch Design”. Sicherheit und Schutz von (personenbezogenen) Daten bilden den Ausgangspunkt beim Entwurf neuer Funktionalitäten und Verbesserungen. Dabei folgen wir unter anderem den folgenden Richtlinien:

- ✓ OWASP Top 10
- ✓ IT-Sicherheitsrichtlinien für Web-Anwendungen des National Cyber Security Centers

Schutz durch Branch Protection

Fellow Digitals nutzt Branch Protection, d.h. Anpassungen des Software-Codes werden immer nach dem Vier-Augen-Prinzip geprüft, bevor sie final umgesetzt werden.

Automatisierte Prüfung

Fellow Digitals verwendet automatisierte Tests von Selemium. Durch die kontinuierliche Durchführung von Regressionstests werden mögliche Fehler frühzeitig erkannt und korrigiert.

Code-Review

Die externe Agentur Securify führt regelmäßig Penetrationstests und White Box Code-Reviews durch. Mit Hilfe von Securify erkennen wir proaktiv Probleme in unserer Software. Und wir bleiben auf dem neusten Stand der Entwicklungen in der Informationssicherheit.

Zusätzlich zu den regelmäßigen internen Sicherheitsaudits und Penetrationstests hilft Fellow Digitals seinen Kunden auch gerne bei eigenen Tests und Penetrationstests.

DDoS-Schutz und Anti-Virus

Denial-of-Service-Angriffe (DDoS) sind leider ein bekanntes Phänomen im Internet. Fellow Digitals verfügt jedoch über ein Intrusion-Detection-System, mit dem diese Art von Angriffen schnell erkannt und eingedämmt werden kann. Im Falle eines DDoS-Angriffs wird der Verkehr über die niederländische nationale Wasstraat (NaWas) umgeleitet und “sauber” geliefert.

Fellow Digitals verwendet täglich aktualisierte Virenscanner, um Gefahren von außen zu minimieren.

Anwendungsspezifische **Vorsichtsmaßnahmen**

Unsere Produkte Fellow Intranet und Fellow LMS erfüllen die höchsten Sicherheitsanforderungen. Beide Produkte sind mit modernen Technologien ausgestattet, um eine sichere Nutzung der Software zu gewährleisten.

Single Sign-on

Die Fellow Digitals-Produkte bieten die Möglichkeit, sich mit Single Sign-on (SSO) anzumelden. Nutzer brauchen sich nur einmal anzumelden und können dann sicher und einfach zwischen den verbundenen Systemen wechseln. Fellow Digitals unterstützt SAML oder OpenID Connect, um u.a. Active Directory zu integrieren.

Zwei-Faktor-Authentifizierung

Fellow Intranet und Fellow LMS unterstützen die Zwei-Faktor-Authentifizierung (2FA). Dies fügt dem Anmeldevorgang einen zusätzlichen Schritt hinzu. Wenn 2FA aktiviert ist, müssen die Teilnehmer zusätzlich zu Nutzernamen und Passwort einen temporären PIN-Code über die Google Authenticator-Anwendung eingeben.

Nutzerberechtigungen und Rollen

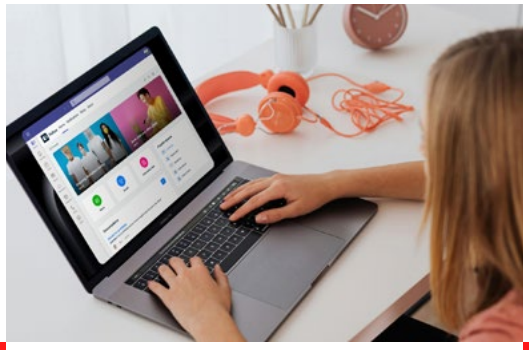
Innerhalb von Fellow Intranet und Fellow LMS haben Sie die Möglichkeit, Berechtigungen für jeden Nutzer festzulegen. Unsere Software verfügt über ein ausgeklügeltes Authentifizierungsmodell, in dem verschiedene Rechte und Rollen unterschieden werden.

Single Sign-on in der Praxis

Im Durchschnitt verbraucht ein Endnutzer bis zu 9 verschiedene Login-Codes für alle Arten von Anwendungen. Dies führt zu Situationen, in denen Mitarbeiter die gleichen Passwörter verwenden und diese an schlecht gesicherten Orten aufbewahren. Das ist etwas, was Sie vermeiden möchten.

Single Sign-on bietet eine Lösung für dieses Problem. Dank offener Standards kann eine sichere Verbindung zwischen Fellow Intranet oder Fellow LMS mit Active Directory hergestellt werden, sodass Sie sich nur einmal mit den gleichen Daten anmelden müssen. Dies ist nicht nur sicherer, sondern auch nutzerfreundlicher.

So ist es möglich, schnell zwischen Fellow Intranet, Fellow LMS und anderen verknüpften Anwendungen, wie Office 365, zu wechseln.



Nutzerrechte in der Praxis

Unsere Plattformen wenden die folgenden Berechtigungsstufen an.

Fellow Intranet/Viadesk

Lesen- Dokumente lesen
Kommentieren - Dokumente lesen und kommentieren
Hinzufügen - Dokumente zur Plattform hinzufügen
Bearbeiten - Den Inhalt von Dokumenten bearbeiten
Verwalten - Alle Verwaltungsfunktionen der Plattform

Fellow LMS/LMS+

Teilnehmer- Teilnahme als Lerner
Assistent - Nutzer- und Registrierungs-verwaltung
Autor - Funktionen zur Erstellung und Verwaltung von Inhalten
Auditor - Überprüfung von Inhalt und Ergebnissen
Trainer - Überprüfung und Feedback geben
Manager - Alle oben genannten Rechte plus Verwaltung der Akademie

Richtlinie für sichere Passwörter

Wenn ein Teilnehmer ein Konto bei Fellow Intranet oder Fellow LMS erstellt, muss dieses eine Reihe von Anforderungen erfüllen. Zum Beispiel die Länge und die Verwendung von Sonderzeichen. Dadurch wird das Konto weniger anfällig für Hacking.

Automatische Kontosperrung

Unser System blockiert automatisch ein Nutzerkonto, wenn die maximale Anzahl falscher Anmeldeversuche erreicht ist.

User-Provisioning-API

Über eine API-Verbindung ist es möglich, User Provisioning zu nutzen. Das bedeutet, dass Teilnehmer auf einfache, aber sichere Weise zur Plattform hinzugefügt und von ihr entfernt werden können.

Audit-Trail-Protokollierung

Die Log-Dateien der Aktivitäten werden auf einem zentralen Server aufbewahrt und sind somit sicher für Audits und mögliche forensische Untersuchungen.

Multi-Tenant-Architektur

In einer Multi-Tenant-Architektur arbeiten mehrere Instanzen einer Anwendung in einer gemeinsam genutzten Umgebung. Diese Technik gewährleistet, dass Kunden die Plattform gleichzeitig sicher nutzen können.

Externe **Prüfungen**

Um sicherzustellen, dass die getroffenen Sicherheitsmaßnahmen die gewünschte Wirkung haben, wird Fellow Digitals regelmäßig von externen Parteien überwacht.

Code-Überprüfungen und Penetrationstests

Das in Amsterdam ansässige Unternehmen Securify führt mehrmals im Jahr verschiedene Arten von Tests durch. Dabei werden Sicherheit und Zuverlässigkeit der Plattform überprüft. Fehler werden gemeldet, damit sie rechtzeitig korrigiert werden können.

- ✓ Penetrationstest (vierteljährlich)
- ✓ White Box Code-Überprüfung (jährlich)

ISO und NEN

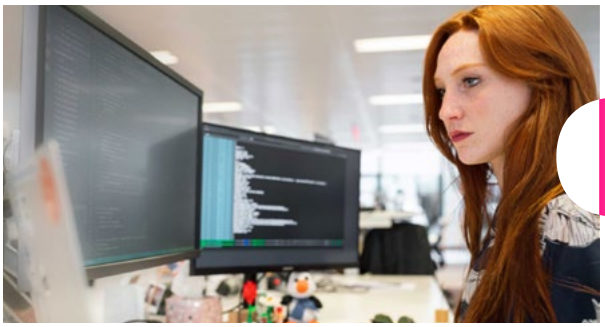
Kiwa ist eine niederländische Organisation für das Testen, Inspizieren und Zertifizieren von Produkten, Systemen und Prozessen. Diese Organisation ist für die jährlichen Audits und die Zertifizierung von Fellow Digitals verantwortlich.

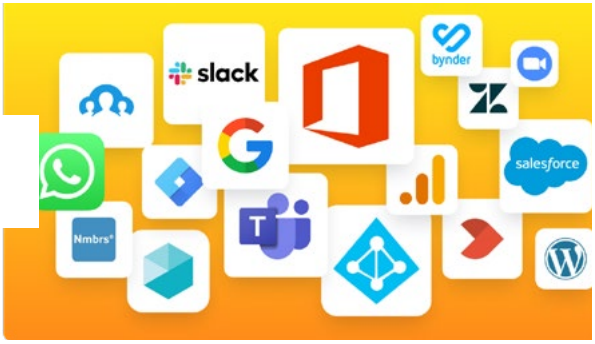
- ✓ ISO 27001
- ✓ ISO 27701
- ✓ NEN 7510

Weitere **Vorkehrungen**

SLA mit 99,9% Uptime

Fellow Digitals bietet seine Dienste mit einem Service Level Agreement (SLA) an. In diesem SLA werden Vereinbarungen über die Qualität unserer Dienstleistungen getroffen. Wir garantieren eine Uptime von 99,9%, was bedeutet, dass Ihre Plattform (fast) immer online verfügbar ist.





REST-API

Mit dem Industriestandard REST-API von Fellow Intranet und Fellow LMS können andere Anwendungen einfach integriert werden. Auf diese Weise wird Ihre Plattform zum Herzstück des digitalen Arbeitsplatzes für alle Betriebs- oder Lernmanagementprozesse.

Haben Sie noch **Fragen?**

Wir freuen uns Ihnen **zu helfen**

Kontaktieren Sie uns über info@fellowdigitals.de
oder rufen Sie uns an: +49 (0)221 828 293 64

Fellow Digitals bv

Amsterdam Office
Weesperplein 4A
1018 XA Amsterdam
Niederlande

T: +31 (0)20 305 76 60
www.fellowdigitals.com
info@fellowdigitals.com

Fellow Digitals GmbH

Köln Office
Brüsseler Str. 25
50674 Köln
Deutschland

T: +49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Bayern Office
Hauptstrasse 48
83684 Tegernsee
Deutschland

+49 (0)221 828 293 64
www.fellowdigitals.de
info@fellowdigitals.de

Fellow Digitals Pte. Ltd.

Singapore Office
1 Paya Lebar Link #04-01,
Paya Lebar Quarter
408533 Singapore

T: +65 9155 4446
www.fellowdigitals.com
info@fellowdigitals.com

Succeeding together

fellow digitals