Informationssicherheit Dyflexis

Version: 4 November 2022
Klassifikation: Extern

ABSENDER
Dyflexis GmbH
Königsallee 27
40212 Düsseldorf
T. +49 211 418 727 00

KONTAKTPERSON 1
Michael Abspoel - CTO
michael.abspoel@dyflexis.com

Inhaltsangabe

1 Einleitung

Ein sicheres Produkt zu liefern ist nicht nur wichtig für das Vertrauen und das Ansehen von Dyflexis, sondern auch notwendig, um die geltenden Gesetze und Vorschriften für die Verarbeitung von personenbezogenen Daten einzuhalten.

Die Plattform von Dyflexis wird ständig weiterentwickelt.

Um den Datenschutz zu gewährleisten und zu verbessern wird hat die Sicherheit der Plattform stets höchste Priorität. Diesbezüglich setzt Dyflexis unter anderem die folgenden Schwerpunkte:

- Kontinuierliches Testen (auf Sprint-Niveau)
- Kontinuierliche und frühzeitige Einbindung von Sicherheits-Feedback zur Verstärkung des Sicherheitsbewusstsein innerhalb des Entwicklerteams
- Aktuelle Einblicke in Risiken und andere Sicherheitsschwerpunkte

Dieses Dokument enthält eine Zusammenfassung der Maßnahmen, die getroffen werden, um Sicherheitsrisiken in der Plattform frühzeitig zu erkennen und zu beheben.

2 Informationssicherheit bei Dyflexis

Die Qualität unserer Produkte und Dienstleistungen und somit die Datensicherheit haben bei uns allererste Priorität.

Dyflexis ist gemäß den neusten (inter-) nationalen Standards für Datensicherheit, Datenschutz und Qualitätsmanagement zertifiziert. Wir sind andauernd mit der Verbesserung unserer Prozesse beschäftigt und sind deshalb stolz, uns zu den ISO 27001:2013 und ISO 9001:2015 zertifizierten Unternehmen zu zählen.
Dyflexis ist außerdem eines der wenigen Unternehmen, dass über die Data-Pro Zertifizierung verfügt.

Mit der Data-Pro-Zertifizierung erfüllt Dyflexis die DSGVO-Verpflichtungen als Auftragsverarbeiter für KMUs.

ISO 27001:2013 - Informationssicherheit

Datenschutz
Wir sind ISO 27001:2013 zertifiziert und erfüllen damit den höchsten internationalen Standard für Informationssicherheit für alle Arten von Unternehmen. Sie können darauf vertrauen, dass Ihre Daten zu jedem Zeitpunkt sicher gespeichert sind. Außerdem verbessern wir ständig unsere Sicherheitsprotokolle, um mit den neuesten Entwicklungen Schritt zu halten.

Vollständige Zertifizierung
Nicht nur unsere Software ist ISO-zertifiziert, sondern auch unsere kompletten Geschäftstätigkeiten sind weitgehend geprüft. Sie können jederzeit darauf vertrauen, dass Ihnen von einer Mitarbeiterin oder einem Mitarbeiter geholfen wird, die oder der ein umfangreiches Sicherheitstraining durchlaufen hat und Ihre Daten vertraulich behandeln wird.

ISO 9001:2015 - Qualitätsmanagement

Qualität
Die ISO 9001:2015 Zertifizierung steht für hohes Qualitätsmanagement. Kunden können stets die beste Qualität von Dyflexis voraussetzen. Unsere Performance wird kontinuierlich evaluiert und für die Optimierung unserer Dienstleistungen genutzt.

Ständige Verbesserung
Selbstverständlich arbeiten wir auch nach dem Erhalt des ISO 9001- Zertifikats daran, uns weiterhin zu verbessern. Wir werden jährlich von einer unabhängigen Wirtschaftsprüfungsgesellschaft überprüft, um sicherzustellen, dass unser Qualitätsmanagement immer auf dem neusten Stand ist.

Data Pro Zertifikat (DSGVO- geprüft)

Datenschutz

Mit dem Data Pro Zertifikat zeigt Dyflexis, dass wir den Datenschutz sehr ernst nehmen. Die Zertifizierung richtet sich an Unternehmen, die personenbezogene Daten für ihre Kunden verarbeiten.

Sicherheit hat erste Priorität

Dyflexis setzt sich weiterhin für die Sicherheit personenbezogener Daten ein und wird sich in regelmäßigen Abständen erneut für das Data Pro Zertifikat prüfen lassen.

2.1 Ansatz für “Agile- Security Testing”

Agile Security Testing wurde speziell eingeführt, weil wir ständig an unserer Plattform und Produkten arbeiten, die wesentliche Bestandteile unseres Geschäfts sind und ein hohes Risikoprofil aufweisen. Das Ziel von Agile Security Testing ist, nachweislich sichere Produkte zu entwickeln, ohne dabei auf die Innovationskraft oder die Lieferschnellheit verzichten zu müssen.

Mit einem direkten Sicherheits-Feedbackloop werden (anstehende) Sicherheitsprobleme frühzeitig signalisiert und erkannt. Wir setzen damit auf vorbeugende Behebung von Sicherheitsrisiken und versuchen so, Nachbesserungsarbeit zu vermeiden. Außerdem stärkt das kontinuierliche Feedback die Kenntnisse über und das Bewusstsein von Sicherheitsrisiken innerhalb der Teams und optimiert die Qualitätssicherung weiter.

Alle Erweiterungen und Änderungen, die an der Dyflexis Plattform auf Coding- und Infrastrukturebene vorgenommen werden, werden durch manuelle und automatisierte Sicherheitskontrollen verifiziert. Durch die Zusammenarbeit mit internen und externen Sicherheitsexperten wird die Sicherheitsexpertise innerhalb der Entwicklerteams immer erweitert. Ziel dieser aktiven Zusammenarbeit ist es, die Sicherheitsqualität unseres Produkts kontinuierlich zu verbessern und die Entwicklerteams noch sicherheitsbewusster zu machen.

Alle zwei Wochen findet ein Treffen statt, damit alle Beteiligten einen aktuellen Überblick über Risiken, deren Status und andere wichtige Daten bezüglich der Prioritätensetzung, Steuerung und Nachvollziehbarkeit haben.

2.2 Jährliche Nullmessung

Jedes Jahr starten wir unseren Arbeitsprozess mit einer Nullmessung der Infrastruktur und des Produkts, um neben den zweiwöchentlichen Sicherheits- Checkups den generellen Sicherheitsstatus festzustellen. Anhand von einem sogenannten „threat modelling“ (Bedrohungsmodellierung) werden Risiken und Maßnahmen ermittelt, die für die Plattform und die eingesetzte Technologie relevant sind. Dies dient als Grundlage für die Weiterentwicklung und die (risikobasierte) Teststrategie. Die Risikoanalyse wird aktualisiert, sobald relevante Änderungen im Umfeld vorgenommen werden.

Im Rahmen einer White-Box-Sicherheitsstudie dienen diese Prozesse als Basis, um das aktuelle Sicherheitsniveau des betreffenden Produkts/der betreffenden Plattform zu ermitteln. Sicherheitslücken und verbesserungsbedürftige Bereiche werden gemeldet, präsentiert und nach Prioritäten geordnet. Auf diese Weise lernt das verantwortliche Team die Details kennen und stellt sicher, dass alle bereits bekannten Probleme verständlich sind. Die daraus folgende OWASP ASV-Qualitätsbewertung, und somit das identifizierten Verbesserungspotenzial bilden den Input für die Roadmap.

2.3 Agile- Security Testing

Nach dem Abschluss der Nullmessung werden alle Änderungen und Erweiterungen anhand von manueller und automatisierter Sicherheits- (Delta-) Codereviews überprüft und getestet.

Damit verhindert wird, dass während Weiterentwicklungen (Sprints) neue Sicherheitsprobleme auftreten, werden Verbesserungspunkte sofort in einem Portal gemeldet, klassifiziert und priorisiert. Das bildet eine äußerst wirksame Methode, um kritische Sicherheitsverletzungen zu verhindern und die Sicherheitsqualität in einem sehr frühen Stadium zu überwachen.

In anderen Worten könnte man sagen, dass durch diese Methode die Bedrohung noch im Keim erstickt wird.

2.4 Unterstützung und Awareness

Bei der Entwicklung von Software treten ständig Sicherheitsfragen auf. Um auf diese schnell zu reagieren, werden Software-Architekten sowie interne und externe Sicherheitsspezialisten in die Entwicklung miteinbezogen.

Aktuelles Wissen über Angriffstechniken und sichere Programmierung ist entscheidend für die Entwicklung sicherer Produkte. Um das zu erreichen, wird das Team während der Entwicklungsphase ständig mit relevantem Feedback versorgt. Bei Bedarf werden auch gezielte Sensibilisierungsmaßnahmen getroffen.

2.5 Infrastruktur und Hosting

Die Infrastruktur von unserer Software wird in einer privaten Cloud gehostet. Als Cloud-Provider benutzen wir hierfür das französische Unternehmen Scaleway. Unsere Server sind redundant und auf ihre Datenserver in Amsterdam aufgeteilt.

Unsere Infrastruktur wird als Code behandelt (“Infrastructure as Code”). Das bedeutet, dass unsere Infrastruktur unter Versionskontrolle ist und als Code (anstatt manueller Prozesse) verwaltet und provisioniert wird. Damit gewährleisten wir, dass wir "on the fly" Server erstellen können, die jederzeit unseren Standards, einschließlich der richtigen Sicherheitseinstellungen, entsprechen.

Darüber hinaus entspricht unsere Infrastruktur mindestens dem CIS Level 1 -Benchmark des „Center for Internet Security“. Außerdem sind die Server, die innerhalb unseres Netzwerkes miteinander kommunizieren, durch WireGuard-Tunnel gesichert.

Scaleway bietet High Availability (HA) als Service an, was für alle betriebskritischen Teile unserer Infrastruktur aktiviert ist- wie zum Beispiel Load Balancers, Webserver und Datenbanken. Jedes Scaleway-Produkt hat eine eigene Produktseite, worin beschrieben wird, was HA genau umfasst. Alle Details zur HA-Datenbank finden Sie hier: https://www.scaleway.com/de/database/.

2.6 Datenbanken und personenbezogene Daten

Wir folgen dem Prinzip der geringsten Privilegien (Principle of Least Privilege- PoLP). Das heißt, dass nur wenige Personen die Berechtigungen haben, auf die Infrastruktur und/ oder die gespeicherten Daten zugreifen zu können. Sollten Produktionsdaten für die Fehlererkennung oder Analyse benötigt werden, werden sie anonymisiert.

Wir verwenden von Scaleway verwaltete Datenbanken, die sowohl nach ISO 27001:2013 als auch nach Health- data hosting (HDS) zertifiziert sind.

Wir haben für jeden Kunden eine eigene Datenbank eingerichtet, womit wir eine strikte Datentrennung gewährleisten. Diese Datenbanken sind auf dieselben (europäischen) Rechenzentren und die dazugehörigen Datenbank-Cluster verteilt.

Eine strenge interne Zugriffskontrolle stellt sicher, dass keine Kundendaten in Nicht-Produktionsumgebungen verwendet werden. Wenn eine bestimmte Kundendatenbank benötigt wird, um ein Problem zu lösen, das nur diesen speziellen Kunden betrifft, verwenden wir einen Datenanonymisierungsdienst, auf den nur unser Entwicklungsteam Zugriff hat. So wird sichergestellt, dass keine Informationen nach außen dringen können. Die Zugriffsliste wird genau wie die Infrastruktur innerhalb des Codes gepflegt.

2.7 Back-ups

Wir verfügen über automatisierte Mechanismen, um von Datenbanken/ Kundendaten Back-ups zu machen, und diese bei Verlust wieder herstellen zu können. Diese Back-ups werden täglich durchgeführt und wöchentlich stichprobenartig getestet. Die Infrastruktur von Dyflexis ist stateless. Maschinen oder Server müssen zu keinem Zeitpunkt auf eine vorherige Transaktion zurückgreifen oder in einen früheren Zustand versetzt werden.

2.8 Datensicherheit

Für die gesamte externe Kommunikation nutzen wir sichere, verifizierte und verschlüsselte Verbindungen, sowie TLS 1.2 oder TLS 1.3. Außerdem fügen wir weitere Verschlüsselungen hinzu, wenn diese nötig sind.

2.9 Kundenanforderung

Die einzige Anforderung, die wir bezüglich Anschlussmöglichkeiten haben, ist eine aktive Internetverbindung. Wenn diese nicht gegeben ist und das Internet nicht funktioniert, ist auch unsere Web-basierte SaaS-Lösung nicht erreichbar.

Unsere App ist mit Android 5 und neueren Versionen sowie iOS 12 und neueren Versionen kompatibel ist.

Für unsere Hardware Stempeluhren benötigen wir einen Kabelanschluss an das Internet. Die Terminals müssen an die folgenden IP-Adressen/Port/Protokoll – Kombinationen angeschlossen werden können:
212.83.146.92, Port: 22717, Protokoll: TCP (Stempelprotokolll)
212.83.146.92, Port: 123, Protokoll: UDP (NTP)
212.83.146.92, Port: 80, Protokoll: TCP (HTTP)

2.10 Wartung

Software-Wartungen werden nur wenn nötig ausgeführt. Das heißt aber nicht, dass unsere SaaS-Applikation während nötiger Wartungen nicht erreichbar ist. Für die Serverkonfiguration benutzen wir Infrastruktur als Code und verwenden daher einen (zero-downtime) Blue-Green Deployment-Mechanismus, um dies zu erreichen.

Falls sich die seltene Situation ergibt, dass Downtime nötig ist, werden wir unsere Kunden per E-Mail alsbald darüber informieren und dafür sorgen, dass die Wartungsarbeiten wenn möglich außerhalb der normalen Arbeitszeiten durchgeführt werden. In dem vergangenen Jahr haben wir keine Wartungsperiode nötig gehabt und gehen davon aus, dass es sich im Falle einer Wartung eher um Minuten als Stunden handeln wird.

2.11 Release-Strategie

Unsere Release-Strategie bezieht sich auf das Motto “release early, release often“, um einen kurzen Feedback-Loop mit unseren Nutzern und Testern und somit auch die höchste Qualität unserer Software gewährleisten zu können. Auf diese Weise können wir die Auswirkungen von Änderungen vorhersehen, bewerten und gegebenenfalls anpassen und verbessern.

Normalerweise releasen wir mindestens einmal pro Tag an Werktagen, mit der Ausnahme von Freitag.

Wir arbeiten mit “trunk-based Development“ und Feature-Toggles, die es ermöglichen, unseren Code mit einer Gruppe von Early Adopters zu testen, sodass der Code gehärtet ist und bei Bedarf produziert werden kann.
Wir halten uns vollständig an das OTAP- Muster und führen für jede Umgebung unterschiedliche Qualitätsprüfungen durch. Wir haben eine Testpyramide, die aus Akzeptanz-, Integrations-, Unit- und Smoke-Tests besteht.