



## DATENSCHUTZ IN DER WEB-APP SPLINT

### EINLEITUNG

Mithilfe von SPLINT wollen wir den Schulalltag, vor allem im Hinblick auf Inklusion, für alle Beteiligten vereinfachen und administrative Hürden minimieren. Dabei verarbeiten wir naturgemäß teils sehr sensible Daten von beteiligten Schüler:innen und Lehrer:innen. Wir verarbeiten jedoch niemals mehr Daten, als zur Erfüllung der Aufgaben nötig!

Diese Übersicht beschreibt, welche Daten wir erheben, sowie wie wir diese schützen. Im Rahmen der Entwicklung wurden von Anfang an die Grundsätze der Datensparsamkeit, Privacy by-Design und Privacy-by-Default konsequent berücksichtigt. Das von uns gewählte Programmiermodell bietet Möglichkeiten, um auf eventuelle zukünftige Veränderungen der Fragebögen flexibel und sicher reagieren zu können.

### WELCHE DATEN WERDEN VON WEM ERHOBEN UND WER EMPFÄNGT DIESE?

Lehrer:innen Stammdaten	Schüler:innen Stammdaten	Empfänger:innen zur Leistungserbringung
- vollständiger Name - Geschlecht - Bundesland in dem sie tätig sind - Berufsstand   Berufsgruppe - E-Mail-Adresse - Unterrichtsfächer	- vollständiger Name - Geschlecht - Geburtsdatum - Schulklasse bzw. Lerngruppe - E-Mail-Adresse	- Schulen (Statistiken via Schul-Account) - Behörden - IT-Dienstleister
Kontoinformation   Kontaktdaten	Ergebnisse	Rechnungswesen   Buchhaltung
- Kreditkartendaten - Bankverbindung - Telefonnummer	- Ergebnisse pädagogischer Beobachtungen für die kooperative Förderplanung	- Rechtsanwält:innen - Steuerberater:innen - Wirtschaftsprüfer:innen - Steuerbehörde

### DATENSCHUTZVORKEHRUNGEN AUF EINEN BLICK

Inklusion Digital	Unsere Partner
- Zwei-Faktor Authentifizierung (freiwillig, verpflichtend wo vorgeschrieben) - Verschlüsselung der Website, App und Transportwege - Zugriff nur für ausgewählte Mitarbeiter und niemals auf Betriebssystemebene - Dezidierte Vergaberechtesteuerung (intern und benutzerseitig)	- Zutrittskontrollsystem (physisch) sowie Zugriffskontrollsystem (systemseitig) - Verpflichtung aller Mitarbeiter auf die Vertraulichkeit gemäß § 52 BDSG - Handlungen ausschließlich auf Weisung des Verantwortlichen - Protokollierung aller Mitarbeiterzugriffe, Zugriffe nur via VPN



## DATENSCHUTZ IN DER WEB-APP SPLINT

### PRIVACY-BY-DESIGN

Alle bei uns sowie unseren Unterauftragnehmern gespeicherten personenbezogenen Daten können stets nur von angemeldeten Nutzer:innen eingesehen werden. Durch unseren Klassenzimmermodus sind alle personenbezogenen Daten nach Anmeldung standardmäßig unleserlich, erst nach manueller Freischaltung werden diese leserlich. Halbjährlich werden außerdem alle angemeldeten Nutzer:innen systemseitig gefragt, ob die zugriffsberechtigten Personen noch aktuell sind - so werden Lehrer:innenwechsel oder aber Klassenwechsel der betroffenen Schüler:innen regelmäßig berücksichtigt.

Falls es nötig sein sollte, dass weitere Nutzer:innen neben dem/der verantwortlichen Nutzer:in auf Förderziele und die damit verbundenen personenbezogenen Daten der Schüler:innen zugreifen müssen, so geht dies nur durch explizite Freigabe durch den/die verantwortliche(n) Nutzer:in. Sollten der/die verantwortliche Nutzer:in nicht an derselben Schule unterrichten, muss darüber hinaus die Identität (Name, Email-Adresse) des/der Nutzer(s):in durch den/die verantwortliche Nutzer:in verifiziert werden.

### ANONYMISIERUNG VON PERSONENBEZOGENEN DATEN

Alle personenbezogenen Daten, die wir im Rahmen der Nutzung unseres Angebotes erheben, werden in verschlüsselter Form, gespeichert. Jede Kommunikation von und zu unseren Systemen ist SSL-Transportverschlüsselt (TLS 1.3). Alle ruhenden Daten sind ebenfalls komplett verschlüsselt (AES 256). Auch bei der Auswahl unseres Serverproviders haben wir darauf geachtet, dass dieser voll nach DSGVO zertifiziert ist und dieselben hohen Anforderungen an Datensicherheit stellt wie wir.

Seitens unseres Serverproviders erhalten nur solche Administratoren Zugang zu unseren Serverkapazitäten, welche explizit mit der Betreuung unserer Services betraut sind nach Art. 32 Abs. 4 DSGVO auf die Vertraulichkeit verpflichtet wurden. Alle Zugänge seitens der Mitarbeiter finden via VPN statt und werden detailliert protokolliert. Allen Zugriffen seitens des Providers liegt unser Berechtigungskonzept zugrunde. Der Grundsatz der Datentrennung wird strikt eingehalten.

Die vollständigen Maßnahmen und Vorkehrungen unseres Server-providers finden Sie unter: [Auftragsverarbeitungs \(AV\)-Vertrag \(planetary-networks.de\)](#). Alle personenbezogenen bzw. potentiell personenbezogenen Daten (z.B. Freitextfelder) im System (von Nutzer:innen | Schüler:innen | Kolleg:innen) sind zusätzlich applikationsseitig verschlüsselt (ChaCha20-Poly1305) und somit auch bei Datenbankvollzugriff nicht lesbar.

Um das Identifizieren von Schüler:innen aufgrund von assoziierten Daten (Profilbildung) unmöglich zu machen, wird die Zuordnung von Schüler:innen zu allen Beobachtungspunkten, konkreten Fördermaßnahmen und assoziierten Personen applikationsseitig verschlüsselt.

### DATENSPARSAMKEIT

Unsere Applikation und unsere gesamte Systemumgebung wurden von Anfang an mit Blick auf zentrale Datenschutzgrundsätze entwickelt. So sind Privacy by Design, also das Berücksichtigen und Priorisieren von Datenschutzaspekten im gesamten Entwicklungsprozess, sowie Privacy by Default, also Datenschutz-freundliche Grundeinstellungen für den jeweiligen Benutzer, für uns selbstverständlich. Ein besonderes Augenmerk legen wir auch auf den Grundsatz der Datensparsamkeit. Wir erheben, sowohl von Lehrer:innen, als auch von Schüler:innen, lediglich solche Daten, die zur Erfüllung unserer Aufgaben Ihnen gegenüber absolut notwendig sind. In keinem Schritt erheben wir optionale Daten oder solche, die für unsere Services abdingbar wären.



## DATENSCHUTZ IN DER WEB-APP SPLINT

### ZUGRIFF AUF DATEN

Die Verteilung der Zugriffsrechte wird durch die anlegenden Pädagog:innen vorgenommen. Der/Die Pädagog:in entscheidet, wer Informationen eines Schülers einsehen darf. Der Zugriff wird granular auf eines oder mehrere Förderziele gewährt. Im Rahmen einer Schul- und einer Schulträgerlizenz, ist es dem Schuladministrator möglich, die Schüler:innen einer Lehrkraft an andere Kolleg:innen der gleichen Schule zu verteilen. Um Missbrauch (Kontrolle durch Vorgesetzte) vorzubeugen, kann dies nur dann gemacht werden, wenn dem Lehrer die Assoziation zur Schule komplett entzogen wird (Langzeit erkrankt, Schulwechsel, verstorben).

Unsere Mitarbeiter haben keinen Zugriff auf personenbezogene Daten der betreuten Schüler, lediglich berechtigte Personen können auf diese verschlüsselten Daten zugreifen. Auch im Falle von notwendigen Wartungs- oder anderen Serverarbeiten haben unsere Mitarbeiter zu keinem Zeitpunkt die Möglichkeit auf Schülerdaten zuzugreifen.

Zu Wartungs- und Supportzwecken haben die Geschäftsführung sowie ausgewählte, besonders sensibilisierte Mitarbeiter Datenbank-Vollzugriff, können aufgrund der oben beschriebenen applikations-seitigen Verschlüsselung jedoch keine personenbezogenen Daten lesen. Daten von registrierten Lehrkräften bzw. Schulen werden ausschließlich zu den vertraglich vereinbarten, gesetzlich legitimierten Zwecken verarbeitet. Eine Verarbeitung darüber hinaus oder gar eine Weitergabe findet nicht statt. Unsere Server sind durch Passwörter zugriffsgesichert und werden täglich durch Backups gesichert. Wir verwenden eine 2-Faktor Authentifizierung für den Zugriff auf unsere Systeme (aktuell freiwillig). Sollte eine solche Authentifizierung in Ihrem Bundesland verpflichtend sein, wird diese standardmäßig auf Ihrem Account aktiviert.

### TRANSPARENZ

Wir wissen um die Sensibilität der uns anvertrauten Daten und behandeln diese daher mit herausragender Sorgfalt. Zu dieser Verantwortung gehört für uns auch eine transparente und nachvollziehbare Kommunikation, weshalb wir Daten erheben und wie diese geschützt sind. Auskunft darüber geben in erster Linie unsere Datenschutzerklärung, sowie der ggf. mit uns geschlossene Auftragsverarbeitungsvertrag. In diesen Dokumenten erläutern wir, weshalb wir welche Daten benötigen, wer diese in unserem Auftrag verarbeitet oder speichert und wie Sie diese Daten löschen lassen können.

Falls darüber hinaus Fragen bestehen freuen wir uns darüber, wenn Sie mit uns in Kontakt treten, am besten per Email an [datenschutz@inklusion-digital.de](mailto:datenschutz@inklusion-digital.de).

### IMPRESSUM

Inklusion-Digital GmbH  
Friedo Scharf, Sebastian Trapp  
[www.inklusion-digital.de](http://www.inklusion-digital.de) | 030 577109191  
[friedo.scharf@inklusion-digital.de](mailto:friedo.scharf@inklusion-digital.de)  
Amtsgericht Charlottenburg  
HRB 222176 B  
Steuernummer 37/359/52072

### URHEBERRECHT

Dieser Newsletter dient der Information und darf für diese Zwecke von der Inklusion-Digital GmbH verwendet werden. Eine unerlaubte Weitergabe oder Vervielfältigung bedarf der Genehmigung der Urheber:innen.

© 2022 Inklusion-Digital GmbH  
All rights reserved.