Sicherheit und Datenschutz

Höchste Priorität – Immer auf dem neuesten Stand

LITTLE BIRD überzeugt beim Datenschutz und wird mit höchster Priorität umgesetzt. Sicherheitsanforderungen von lokalen, regionalen, landesweiten und kirchlichen Datenschützern und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) werden stetig in die Konzeption und Entwicklung einbezogen, überprüft und aktualisiert. Sämtliche Daten werden nach der Europäischen Datenschutzgrundverordnung (DSGVO) verarbeitet und von beauftragten Datenschutzunternehmen kontrolliert.

LITTLE BIRD besteht aus zwei Elementen, die getrennt voneinander abgesichert sind:

- Elternportal für Registrierung, Anmeldung, Platzanfragen und Kommunikation. Die erfassten und versendeten Anmeldedaten können sofort danach komplett gelöscht werden.
- Verwaltungssoftware als Arbeitsplattform für Kitas, Träger und Jugendamt. Kein Zugriff durch Eltern möglich und nur per zusätzlicher Zertifikatsinstallation nutzbar.

Beide Elemente verfügen jeweils über entsprechende Datenschutzpakete und tauschen im Prozess nach festgelegten Sicherheitsegeln laufend relevante Informationen miteinander aus.

Allgemeine Schutzmaßnahmen in Elternportal und Verwaltungssoftware*

- Verschlüsselung des Datenverkehrs
- Dezentrale Datenspeicherung
- Trennung zwischen Portal- und Verwaltungsdaten
- Schutz vor Datendiebstahl
- Mehrstufige Datenbank-Backup-Strategien
- Hosting in zertifizierten Rechenzentren in Deutschland

* Eine detaillierte Darstellung der Sicherheitspakete gibt es auf der Rückseite

LITTLE BIRD GmbH
Landsberger Allee 131a
10369 Berlin
www.little-bird.de

Sprechen Sie uns gerne an:
Tel.: +49 30 9120656-0
Fax: +49 30 9120656-215
E-Mail: info@little-bird.de

Mitglied bei:

Initiative D21 bitkom

LITTLE BIRD - Datenschutz
So viel Sicherheit muss sein

Die Anwendungen von LITTLE BIRD verwenden u.a. die folgenden Sicherheitsmerkmale:

	VERWALTUNGSSOFTWARE	ELTERNPORTAL
Hosting Sowohl Elternportal als auch Verwaltungssoftware werden ausschließlich in ISO 27001 und ISO 9001 zertifizierten Rechenzentren in Deutschland gehostet.	✓	✓
SSL-Zertifikate (https) Ermöglicht sichere transportverschlüsselte Kommunikation zwischen Anwender und Webserver zur abhörsicheren Übertragung von Daten.	✓	✓
HTTP Strict Transport Security (HSTS) Ein Sicherheitsmechanismus für HTTPS-Verbindungen, der dem Browser des Anwenders mitteilt, in Zukunft ausschließlich verschlüsselte Verbindungen für diese Domain zu nutzen.	✓	✓
Perfect Forward Secrecy (PFS) Sicherheitsverfahren um zu verhindern, dass durch Bekanntwerden eines geheimen TLS/SSL - Sitzungsschlüssels die zukünftige und auch vergangene Kommunikation entschlüsselt werden kann.	✓	✓
Client-Zertifikate (zur Zwei-Faktor-Identifizierung) Mit den Zertifikaten (dem zweiten Faktor Nutzername/ Passwort) werden Nutzer eindeutig authentifiziert.	✓	
Mehrstufiges Berechtigungskonzept Nutzer des Systems (Lizenz-Nutzer) dürfen nur die Daten einsehen und bearbeiten, die für ihre Tätigkeit notwendig sind.	✓	
Authentifizierung beim Zugriff auf Verwaltungsdaten Ausschließlich Nutzer mit vom System ausgestellten Zertifikaten haben Zugriff auf bestimmte sensible personen- und vertragsbezogene Daten.	✓	
Verschlüsselte Datenbank Personenbezogene Daten werden auf dem Datenbank-Server zusätzlich verschlüsselt gespeichert.		✓

Version 2020-11-1