

Audit Prüfbericht | Executive Summary

Prüfer: Dr. David Rump

Berlin, den 08.04.2021

DSGVO Audit Prüfbericht

Little Bird GmbH – Kita & Elternportal

Zusammenfassung

Die turnusmäßige Überprüfung der Little Bird GmbH, der von ihr betriebenen Software (Kita- und Elternportal), sowie der internen Organisation und Infrastruktur in Bezug auf die Verarbeitung von personenbezogenen Daten ergibt, dass die Little Bird GmbH datenschutzrechtlich, gemessen an den gesetzlichen Anforderungen der DSGVO, gut aufgestellt ist. Die bestehende interne Datenschutz-Organisation bzw. das Datenschutzmanagementsystem wurde im Laufe des Jahres 2021 systematisch weiter fortentwickelt und optimiert, wie nachfolgend erläutert.

Insgesamt ist zu erkennen, dass die gesetzlichen Anforderungen an den unternehmerischen Datenschutz erfüllt sind. So werden die Grundsätze der Verarbeitung von personenbezogenen Daten, insbesondere Transparenz, Treu und Glauben, Zweckbindung und Datenminimierung entsprechend beachtet. Es werden grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet.

Fux Legal
Krausnickstr. 10
10115 Berlin
fon 030 288 860 60
fax 030 288 860 61

hallo@fux-legal.de

Dr. David Rump

Rechtsanwalt
Datenschutzbeauftragter (TÜV)

Stefan Pflug

Rechtsanwalt | Mediator (DAA)
Fachanwalt für Arbeitsrecht
Wirtschaftsmediator

Bankverbindung

Oldenburgische Landesbank
Konto: 5046 2332 00
BLZ: 280 200 50
IBAN: DE31 2802 0050 5046 2332 00
BIC: OLBODEH2XXX

UST-ID

DE318761911

Zur Gewährleistung dieser Grundsätze definiert und implementiert das interne Datenschutzmanagementsystem ein umfangreiches Datenschutz- und IT-Sicherheitskonzept, welches technische und organisatorische Maßnahmen als tragenden integralen Bestandteil bestimmt, die den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DSGVO genügen. Dazu zählen:

- Eine Datenschutzleitlinie sowie verbindliche Unternehmensregelungen und Steuerung von Prozessen.
- Regelungen und Leitlinien für datenschutzrelevante Prozesse,
- Verpflichtung und Schulung aller Mitarbeiter zur Steuerung der Prozesse.
- Eine Verarbeitungsübersicht nach Maßgabe von Art. 30 Abs. 1 DSGVO,
- Verträge mit Auftragsverarbeitern nach Maßgabe von Art. 28 DSGVO.

Die Mitarbeiter sind hinsichtlich der für sie relevanten Bestimmungen zum Datenschutz geschult und im Umgang mit personenbezogenen Daten sensibilisiert.

Das Datenschutzmanagementsystem bestimmt zudem einen Zyklus zur Fortentwicklung, um die kontinuierliche Verbesserung der Prozesse und Prüfung und Weiterentwicklung dieser Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sicherzustellen.

Die Software erfüllt die Anforderungen nach Privacy by Design und Privacy by Default nach Artikel 25 DSGVO. So können Kunden ihre Pflichten als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO und insbesondere die Rechtmäßigkeit der Datenverarbeitung in eigener Verantwortung sicherstellen.

So wird den Kunden ermöglicht, zusätzliche Einstellungen und Maßnahmen zu treffen, um die Software den eigenen datenschutzrechtlichen Bedürfnissen anzupassen, bspw. indem der Umfang der Verarbeitung personenbezogener Daten selbst gesteuert wird. Außerdem können Zugriffsrechte entsprechend eines internen Berechtigungskonzeptes selbst gesteuert und konfiguriert

werden, um sicherzustellen, dass die nutzenden Personen nur Zugriff auf die für sie relevanten Daten erhalten und Unbefugte von dem Zugriff ausgeschlossen werden.

Little Bird hat zudem interne Prozesse sowie software-seitige Maßnahmen implementiert, um die Rechte der Betroffenen umfänglich gewährleisten zu können. So wird dem Kunden ermöglicht, entsprechende Begehren zügig und bequem zu erledigen. Beispielhaft zu nennen sind hierzu insbesondere die Möglichkeiten der Datenlöschung, Sperrung sowie Auskunft und Berichtigung.

Die softwareseitigen Prozesse sowie sonstigen technischen und organisatorischen Maßnahmen werden gegenüber den Kunden in einem Vertrag über die Auftragsverarbeitung verbindlich vereinbart.

Zusammenfassend kann festgehalten werden, dass die Software in ihrer Konstruktion, dem Betrieb und der Umsetzung die Anforderungen der europäischen Datenschutz Grundverordnung (DSGVO) umfassend erfüllt. Die dem zugrunde liegenden Prozesse und Maßnahmen werden fortlaufend überprüft und angepasst.

Dr. David Rump

Rechtsanwalt

Datenschutzbeauftragter (TÜV)

