Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)

Inhalt

A. Stammdatenblatt

Name und Kontaktdaten des Plattformanbieters

a. **Name(n) und Anschrift(en):**
   Fox Education Services GmbH
   Liechtensteinstraße 25
   1090 Wien

b. **E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):**
   support@foxeducation.com

c. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten:**
   Dr. Mario Schnakl
   Ploil Boesch Rechtsanwälte GmbH
   Stadiongasse 4
   1010 Wien
   datenschutz@foxeducation.com

d. **Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des Anbieters:**
   David Schalkhammer
   Geschäftsführer der Fox Education Services GmbH
   ds@foxeducation.com

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung:

1. Erbringung vertraglich vereinbarter IT-Leistungen, durch die eine sichere Kommunikation, Organisation und Kollaboration zwischen Schulleitung, Eltern, Lehrer*innen, Schüler*innen und sonstigen Stakeholdern gewährleistet werden soll

2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Ja ☐ **Nein** ☒

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?

Gemäß Art 35 DSGVO ist die Durchführung einer Datenschutz-Folgenabschätzung dann erforderlich, wenn die beabsichtigten und/oder die laufenden Datenverarbeitungen mit einem überdurchschnittlich hohen Risiko einer Verletzung von Betroffenenrechten behaftet sind. Ein solches (erhöhtes) Risiko besteht im konkreten Fall nicht, zumal keine neuartigen Technologien zum Einsatz kommen und auch keine (sensiblen bzw. strafrechtlich heiklen) Daten im Sinne der Art 9 Abs 1 und 10 DSGVO verarbeitet werden. Die Datenverarbeitung erfolgt zudem weder in einem besonderen Ausmaß noch Umfang. Weiters werden keine besonderen Formen oder Wege der Datenerhebung genutzt. Zudem ist gemäß Artikel 35 Absatz 1 DSGVO nicht der Auftragsverarbeiter selbst, sondern der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet, wenn eine solche notwendig wäre.

C. Detailangaben zu (1) Erbringung vertraglich vereinbarter IT-Leistungen, durch die eine sichere Kommunikation, Organisation und Kollaboration zwischen Schulleitung, Eltern, Lehrer*innen, Schüler*innen und sonstigen Stakeholdern gewährleistet werden sollen

1. Kategorien der betroffenen Personen

1. Pädagog*innen (im weitesten Sinne; erfasst auch Lehrkräfte, Sporttrainer*innen, außerschulische Betreuungspersonen, Unterstützungspersonal, etc.)
2. Schulleitung und Vertreter*innen von Trägerorganisationen
3. Eltern/Schüler-Nutzer*innen (im weiteren Sinne; erfasst auch weitere erziehungsberechtigte und nicht erziehungsberechtigte Bezugspersonen von Schüler*innen)
4. Schüler*innen (Stammdaten)

2. **Rechtsgrundlagen**

Art 6 Abs 1 lit a DSGVO - Einwilligung
Art 6 Abs 1 lit b DSGVO - Vertragserfüllung
Art 6 Abs 1 lit e DSGVO - Wahrnehmung von im öffentlichen Interesse liegenden Aufgaben (durch die Gewährleistung einer sicheren Kommunikation, Organisation und Kollaboration zwischen Schulleitung, Eltern, Lehrer*innen, Schüler*innen und sonstigen Stakeholdern)

3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt: (freiwillig)

Zustimmungserklärungen sind in der Nutzerdatenbank abgelegt.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen

a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Server-Host (Apps)	IT Security (Apps)	Server-Host (Website)	E-Mail-Dienst	SMS-Dienst
1-3	1	Name*	Nein	x	x	x	x	
	2	Anrede*	Nein	x	x			
	3	Kontaktdaten (E-Mail*, Telefonnummer)	Nein	x	x	x	x	x
	4	Interne Nutzer-ID*	Nein	x	x			
	5	Bevorzugte Übersetzungssprache*	Nein	x	x			
	6	Zuordnung zu Klasse oder Kind*	Nein	x	x			
	7	IP-Adresse*	Nein	x	x	x		
4	8	Name*	Nein	x	x			
	9	Geschlecht	Nein	x	x			
	10	Geburtsdatum	Nein	x	x			
	11	Wohnadresse	Nein	x	x			
	12	Schulstufe	Nein	x	x			
	13	Notizen durch Lehrpersonal/Eltern	Nein	x	x			
	14	Mitteilungen von Lehrpersonal/Eltern*	Nein	x	x			
	15	Zuordnung zu Klasse*	Nein	x	x			

	16	Verbundene Eltern*	Nein	x	x			
1-4	17	Video- und Ton	Nein	x	x			

*notwendig

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1; 6; 8; 14-16	Gesetzliche Aufbewahrungspflicht von 3 Jahren (wie elektronisches Klassenbuch) sofern keine regionalen gesetzlichen Regelungen kürzere Aufbewahrungsfristen vorsehen.
7	Die IP-Adresse des/der Nutzer*in wird nicht gespeichert, sondern lediglich während der Nutzung verarbeitet.
17	Aufbewahrung nur während der Nutzung der Funktion. Daten werden nach Beendigung des Video-Calls gelöscht.
2-5; 9-13	Bis zur Beendigung der Geschäftsbeziehung

5. Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung),

Empfängerkategorien (aus 4.a.)	Name des Empfängers
Server-Host (Apps/Website)	Exoscale Cloud Hosting, Boulevard de Grancy 19A, 1006 Lausanne, Schweiz *member of* A1 Telekom Austria Group, Lassallestraße 9, 1020 Wien, Österreich
IT-Security (Apps)	Link11 GmbH, Lindleystraße 12, 60314 Frankfurt am Main, Deutschland
E-Mail-Benachrichtigungs-Dienst	rapidmail GmbH, Augustinerplatz 2, 79098 Freiburg i.Br., Deutschland
SMS-Benachrichtigungs-Dienst	sms.at mobile internet services GmbH, Brauquartier 5/13, 8055 Graz, Österreich

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit:

i. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:
   - 24/7 Portier
   - Elektronische Zutrittskontrolle mit biometrischer Identitätsfeststellung
   - Videoüberwachung
   - Alarmanlage mit Bewegungsmelder

ii. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, durch
   - Nutzung starker Kennwörter (einschließlich entsprechender Policy)
   - Verschlüsselung von at-rest Daten
   - Verwendung von State-of-the-art Software-Sicherheitsmechanismen
   - Strikte IP-Beschränkung für Datenbankzugang

iii. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, durch
   - Protokollierung von Zugriffen
   - Datenfreigabe auf Basis streng definierter Authorisierungsregeln (Nutzer-Rollen)

b. Integrität:

i. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung personenbezogener Daten.

ii. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, Protokollierung der Vorgänge;

c. Verfügbarkeit und Belastbarkeit:

i. Verfügbarkeitskontrolle: Redundante Energieversorgung, Netzwerk und Speicherung verhindern Hardware-bezogene Ausfälle. Systeme werden durch Firewalls isoliert. Online und Offline Backups verhindern Zerstörung oder Verlust von Daten.

d. Pseudonymisierung und Verschlüsselung:

i. Die Datenverarbeitung erfolgt pseudonymisiert, sodass Datensätze nicht ohne weitere Informationen einer Person zugeordnet werden können. Diese Informationen werden separat gespeichert.

e. Evaluierungsmaßnahmen:

i. Datenschutz-Management: regelmäßige Überprüfung der Server-seitigen Verarbeitungsprozesse von personenbezogenen Daten, Überprüfung von Wiederherstellungsszenarien und Mitarbeiterschulungen.