Vereinbarung über die Verarbeitung personenbezogener Daten von Schülern und Eltern im Auftrage

zwischen der

Realschule Mausbach
Im Hahn3
5224 Stolberg

Vertreten durch die Schulleitung im Folgenden "SCHULE" genannt und der Firma

PEDAV Software für Schulen und Kommunen GmbH & Co. **KG**
Lahnbeckestr. 2
45307 Essen

vertreten durch den Geschäftsführer im

Folgenden "PEDAV" genannt

wird folgende Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (Auftragsdatenvereinbarung) geschlossen:

Präambel

Die Firma PEDAV stellt der SCHULE die onlinebasierte Webanwendung "OTIS" Verfügung. Mit dieser Anwendung werden nur zweckdienliche Informationen zwischen der Schule und Schüler-Eltern ausgetauscht. Zweck ist die Verwaltung von Elternsprechtagen und Anmeldungen. Es werden ausschließlich die gemäß der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) zugelassenen Individual- und Organisationsdaten erhoben. Rechtliche Grundlage für die Datenerhebung ist das Schulgesetz NRW-SchuiG (vor allem die in §§ 120 und 122 SchuiG) nebst die dem Schulgesetz zugrunde liegenden weiteren Vorschriften.

Die Firma PEDAV wurde vor 30 Jahren gegründet. Sie versorgt und betreut Schulen mit Schulverwaltungssoftware aus allen Schulformen und Bundesländern. Bei dieser Schulverwaltungs- und der Schulträgersoftware handelt es sich teils um Eigenentwicklungen und teils um bewährte Produkte von Partnern.
Durch Produktqualität und Zuverlässigkeit wird die Schulverwaltungssoftware der Firma PEDAV in Nordrhein-Westfalen und anderen Bundesländern an vielen Schulen eingesetzt.

Gespeichert werden die mittels "**OTIS**" erhobenen Daten bei der **Host Europe GmbH** in Köln. Dieser Provider ist nach ISO 27001, einer internationalen Sicherheitsnorm, zertifiziert. Außerdem verfügt das Unternehmen über ein TÜV-geprüftes Informationssicherheits-Management-System, das den optimalen Schutz der Daten garantiert. Da sich alle technischen Anlagen in Köln befinden, ist gewährleistet, dass sich die Datenverarbeitung ausschließlich nach den Rechtsnormen der BRD bzw. von NRW richtet.

1. **Verantwortlichkeit für die Datenverarbeitung**
   Die SCHULE bleibt als Auftraggeber der Datenverarbeitung für die Einhaltung der Vorschriften des Landesdatenschutzgesetzes NRW (DSG NRW) verantwortlich. Sie ist verantwortliche Stelle im Sinne dieses Gesetzes. Rechte betroffener Personen auf Auskunft, Unterrichtung, Berichtigung, Sperrung oder Löschung sowie vergleichbare Rechte sind gegenüber der SCHULE als "Herrin der Daten" geltend zu machen.

2. **Weisungsgebundenheit**
   Die SCHULE beauftragt die Firma PEDAV die vereinbarten Funktionen des "OTIS"-Systems auszuführen und die darin enthaltenen personenbezogenen Daten zu verarbeiten. Veränderungen und/oder Ergänzungen des Funktionsumfangs für einen neuen Verarbeitungszyklus, bedürfen einer neuen schriftlichen Vereinbarung zwischen SCHULE und PEDAV. Kommt eine solche neue Vereinbarung nicht bis zum 31.03. eines Jahres zustande, so endet diese Vereinbarung, ohne dass es einer Kündigung bedarf, zum Ende des Verarbeitungszyklus automatisch. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

   Weisungsberechtigte Personen des Auftraggebers sind:
   - Frau Jacqueline Marr

   Weisungsempfänger bei PEDAV sind:

   - Herr Reinhold Kuhn
   - Herr Martin Wippersteg

3. **Technische und organisatorische Maßnahmen**
   Die Firma PEDAV gewährleistet die ordnungsgemäße Durchführung der notwendigen technischen und organisatorischen Maßnahmen, soweit sie im Verantwortungsbereich der Firma PEDAV liegen. Für die organisatorische Durchführung der im Verantwortungsbereich der SCHULE liegenden Maßnahmen trägt diese selbst Sorge.

4. **Löschung und Sicherheitskopie**
   Spätestens mit dem Ende eines Verarbeitungszyklus (Ende März eines Jahres) oder bei Beendigung des Vertragsverhältnisses, werden die Schülerdaten aus dem der Anwendung zugrunde liegenden Datenbanksystem gelöscht.

Vor der Löschung wird zum Zweck der Dokumentation für den Archivierungszeitraum von einem Jahr eine Sicherungskopie durch die SCHULE angelegt Die zugehörige Programmversion wird ebenfalls für diesen Zeitraum gesichert (durch die Firma PEDAV). Nach Ablauf des Archivierungs-Zeitraumes werden auch die archivierten Daten gelöscht. Der Zugriff auf die Daten der Sicherungskopie erfolgt durch die SCHULE oder anderer rechtlich zwingender Instanzen nur für Fälle der Beweissicherung oder Revision und nur in den Räumen der Schule.

5. **Besondere Berücksichtigung der Eignung des Auftragnehmers**
   Die SCHULE nutzt seit langem Produkte der Firma PEDAV und ist mit dieser regelmäßig in Kontakt. Die Firma PEDAV ist geeignet, auch für die SCHULE die beschriebene Auftragsdatenverarbeitung durchzuführen.

6. **Unterrichtung der zuständigen Datenschutzkontrolle**
   Die SCHULE unterrichtet den bestellten behördlichen Datenschutzbeauftragten über die Einrichtung und Änderung des vereinbarten DV-Verfahrens. Dieser trägt für die Durchführung der Vorabkontrolle Sorge.

7. **Sonstiges**
   Die Firma PEDAV erklärt, die jeweils gültigen gesetzlichen Regelungen zum Datenschutz einzuhalten. Im Falle von Beanstandungen zum Datenschutz wird die Firma PEDAV die SCHULE darüber in Kenntnis setzen.

   Zur Erhöhung der Sicherheit ist die Aufgabenwahrnehmung bei der Firma PEDAV auf wenige Mitarbeiter begrenzt.

Diese Vereinbarung kann zum Ablauf der Zeitlizenz von beiden Seiten gekündigt werden. Darüber hinaus ist eine außerordentliche Kündigung aus besonderen Gründen möglich.

Datum:	Datum:
Für die SCHULE	Für die Firma PEDAV
	
Schulleitung	Geschäftsführer

Anlage:

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

"**PEDAV**" - PEDAV Software für Schulen und Kommunen GmbH & Co. KG"
Lahnbeckestrasse 2, 45307 Essen
www.pedav.eu

Stand
Mai 2018

1. Pseudonymisierung

- Maßnahmen zur Pseudonymisierung bei gegebener Verhältnismäßigkeit und Umsetzbarkeit

2. Verschlüsselung

- Bereitstellung und Nutzung verschlüsselter Verbindungen per HTTPS
- Verschlüsselung der Identifikationsmerkmale "Nachname, Vorname, Geburtsdatum" in der Datenbank

3. Gewährleistung der Vertraulichkeit

3.1. Zutrittskontrolle

- Zutrittsgeschützte Büroräume

3.2. Zugangskontrolle

- Login mit Benutzername + Passwort
- Anti-Viren-Software für Server, Clients und mobile Geräte
- Einsatz von Firewalls

3.3. Zugriffskontrolle

- regelmäßige Überprüfung/Aktualisierung der Berechtigungen
- Schutz der Rechner durch Startkennwort und Sperrbildschirm mit Kennwort

3.4. Trennungskontrolle

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- getrennte Speicherung von Firmendaten (Buchhaltung, Personalverwaltung etc.)

4. Gewährleistung der Integrität

4.1. Weitergabekontrolle

- alle Mitarbeiter sind vertraglich auf das Datengeheimnis verpflichtet
- bei externer Kommunikation werden Verschlüsselungen nach dem Stand der Technik eingesetzt, sofern der Kommunikationspartner dies unterstützt.
- Löschfristen entsprechen den gesetzlichen Vorgaben
- verschlüsselte Übertragung (SFTP, FTPS, HTTPS)

4.2. Eingabekontrolle

- Es existieren klare Zuständigkeiten für Eingabe, Änderung und Löschung von Daten
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

5. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme

- vgl. unten: Technische und organisatorische Maßnahmen des Hosting-Providers HostEurope GmbH
- Backup & Recovery-Konzept

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- tägliche Datenbank-Backups
- Dokumentierter Prozess für die Wiederherstellung der Daten nach einem Zwischenfall

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1. Datenschutz-Management

- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- mindestens jährliche Sensibilisierung der Mitarbeiter bzgl. Informationssicherheit.
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach, die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.