



Vereinbarung zur Auftragsverarbeitung

Vereinbarung gemäß Art. 28 DSGVO zwischen dem/der

- nachfolgend „Verantwortlicher“ -

und der

we do code UG (haftungsbeschränkt), Blumenstraße 32, 65366 Geisenheim

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

§ 1 Gegenstand der Vereinbarung

- (1) Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden.
- (2) Der Auftrag umfasst folgende Leistungen durch den Auftragnehmer:
 - Betreiben der PROWO-Software für verschiedene Wahlen an der Schule des Verantwortlichen.
 - Anwenden von Änderungen jeglicher Daten innerhalb der Datenbank, welche durch die Software genutzt wird.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien betroffener Personen

- (1) Art und Zweck der Verarbeitung ist die Bereitstellung und Verwaltung einer Software zur Durchführung von schulinternen Wahlen insbesondere Projektwochen.
- (2) Folgende Datenarten oder -kategorien sind Gegenstand der Verarbeitung durch den Auftragsverarbeiter:
 - Notwendige Kommunikationsdaten wie die IP-Adresse.
 - Schülerinnen und Schüler:
 - Vor- und Nachname
 - E-Mail-Adressen
 - Klasse & Jahrgang
 - Lehrer und Lehrerinnen:
 - Vor- und Nachname
 - Geschlecht
 - E-Mail-Adresse
 - Klasse bzw. Stammkurs

§ 3 Pflichten und Rechte des Verantwortlichen

- (1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Verantwortliche verantwortlich. Der Verantwortliche kann jederzeit die

Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

- (2) Der Verantwortliche erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und schriftlich festzulegen.
- (3) Der Verantwortliche hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen sind schriftlich zu bestätigen. Die weisungsberechtigten Personen des Verantwortlichen und die Weisungsempfänger beim Auftragsverarbeiter werden in der Anlage 1 mit Name und Kontaktdaten benannt.

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen und insoweit die Anlage 1 entsprechend zu aktualisieren.

- (4) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 4 Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, es sei denn, es liegt ein Anwendungsfall von Art. 28 Abs. 3 lit. a DSGVO vor. Er verwendet die zur Datenverarbeitung überlassenen personenbezogenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Er beachtet die Bestimmungen der DSGVO und des Landesdatenschutzgesetzes Rheinland-Pfalz (LD SG) und unterwirft sich hinsichtlich der in diesem Vertrag vereinbarten Leistungen der Kontrolle des Landesbeauftragten für den Datenschutz. Ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.
- (2) Der Auftragsverarbeiter sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen sowie die Trennung der Daten des Verantwortlichen von sonstigen Datenbeständen des Auftragsverarbeiters zu.
- (3) Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in das Verzeichnis von Verarbeitungstätigkeiten, die gespeicherten Daten und die Datenverarbeitungsprogramme einschließlich einer Inspektion beim Auftragsverarbeiter.
- (4) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erfor-

derlichen Datenschutz-Folgenabschätzungen des Verantwortlichen hat der Auftragsverarbeiter im notwendigen Umfang mitzuwirken und den Verantwortlichen soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

- (5) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Verantwortlichen datenschutzgerecht vernichtet werden.
- (6) Nach Abschluss der vertraglichen Arbeiten hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen.

Seitens des Verantwortlichen elektronisch zur Verfügung gestellte Informationen sowie etwaige Testdaten sind nach erklärter Abnahme der Leistung zu löschen. Die Löschung erfolgt derart, dass eine Reproduktion nach dem Stand der Technik nicht möglich ist. Die Löschung bzw. Vernichtung ist dem Verantwortlichen schriftlich zu bestätigen.

- (7) Die Beauftragung von weiteren Auftragsverarbeitern ist nur nach vorheriger schriftlicher Genehmigung des Verantwortlichen zulässig. Der Subunternehmer ist ebenfalls sorgfältig unter besonderer Berücksichtigung der Eignung sowie der von ihm getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO auszuwählen.
- (8) Der Verantwortliche ist über wesentliche Veränderungen, die die Art der Datenverarbeitung betreffen, rechtzeitig zu unterrichten. Für den Datenschutz oder die Informationssicherheit erhebliche Entscheidungen zur Organisation und Durchführung der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Verantwortlichen abzustimmen.

§ 5 Datengeheimnis

- (1) Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten für den Verantwortlichen das Datengeheimnis gemäß § 8 LDSG zu wahren. Er verpflichtet sich weiter, über Informationen, die ihm im Rahmen des Auftrags zur Kenntnis gelangen, gegenüber Dritten Verschwiegenheit zu wahren. Die Verschwiegenheitspflicht besteht auch nach Erfüllung des Auftrags weiter.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle

- (1) Der Auftragsverarbeiter verpflichtet sich, die nach Art. 32 DSGVO erforderlichen technisch-organisatorischen Maßnahmen zu treffen und zu dokumentieren. Die technisch-organisatorischen

Maßnahmen sind dem Verantwortlichen zur Verfügung zu stellen. Ist eine Zurverfügungstellung, insbesondere aus Gründen der Informationssicherheit oder der Geheimhaltung ganz oder teilweise nicht möglich, so stellt der Auftragsverarbeiter dem Verantwortlichen die relevanten Auszüge zur Einsichtnahme beim Auftragsverarbeiter zur Verfügung.

Eine Übersicht der verbindlichen technischen und organisatorischen Maßnahmen ist unter Anlage 2 aufgeführt.

- (2) Der Auftragsverarbeiter beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung.
- (3) Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses im Hinblick auf ihre Wirksamkeit regelmäßig zu überprüfen, zu bewerten und zu evaluieren (Art. 32 Abs. 1 lit. d DSGVO). Änderungen dürfen die vereinbarten Sicherheitsstandards nicht unterschreiten. Wesentliche Änderungen sind schriftlich zu vereinbaren.
- (4) Soweit die beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen den Anforderungen des Verantwortlichen nicht genügen, benachrichtigt er den Verantwortlichen unverzüglich. Entsprechendes gilt für Störungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten. Er unterrichtet den Verantwortlichen unverzüglich, wenn eine vom Verantwortlichen erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Verantwortlichen geändert oder ausdrücklich bestätigt wird.

§ 7 Vertragsdauer

- (1) Der Vertrag beginnt am _____ und endet am _____.
- (2) Der Verantwortliche kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen die Bestimmungen der DSGVO und anderer Datenschutzvorschriften oder dieses Vertrages vorliegt.

§ 8 Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer möglichen Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO meldet der Auftragsverarbeiter dies unverzüglich, damit der Verantwortliche in die Lage versetzt wird, die Meldefrist von 72 Stunden gegenüber der zuständigen Aufsichtsbehörde einzuhalten.

§ 9 Haftung

- (1) Der Auftragsverarbeiter haftet - sofern diese Vereinbarung zur Auftragsverarbeitung keine anderslautenden Regelungen treffen - gleich aus welchem Rechtsgrund nur für Vorsatz und grobe Fahrlässigkeit. Diese Haftungsbeschränkung gilt auch für seine Erfüllungs- und Verrichtungsgehilfen.
- (2) Für leichte Fahrlässigkeit haftet der Auftragsverarbeiter nur bei der Verletzung vertragswesentlicher Pflichten. In diesem Fall ist jedoch die Haftung für mittelbare Schäden, Mangelfolgeschäden und entgangenen Gewinn ausgeschlossen. Die Haftung für positive Forderungsverletzung, Verschulden bei Vertragsschluss und aus unerlaubter Handlung ist außerdem auf den Ersatz des typischen, vorhersehbaren Schadens begrenzt.
- (3) Die Haftungsbeschränkungen aus den Absätzen 1 und 2 gelten nicht für die Verletzung von Leben, Körper und Gesundheit.

§ 10 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverarbeiter, wird er die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragsverarbeiter unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 11 Sonstiges

- (1) Sollte das Eigentum des Verantwortlichen beim Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen.
- (2) Änderungen oder Ergänzungen zu diesem Vertrag sind nur wirksam, wenn sie schriftlich vereinbart werden. Dies gilt auch für eine Änderung dieser Schriftformklausel. Satz 1 gilt nicht für Anpassungen bezüglich der weisungsberechtigten Personen sowie Weisungsempfänger (Anlage 1).
- (3) Nebenabreden wurden nicht vereinbart.

§ 12 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Für den Verantwortlichen:

(Vorname)

(Nachname)

(Datum)

(Ort)

(Unterschrift und Dienstsiegel)

Für den Auftragsverarbeiter:

Simon

(Vorname)

Kolb

(Nachname)

(Datum)

(Ort)

Julius

(Vorname)

Settili

(Nachname)

(Datum)

(Ort)

(Unterschrift)

Anlage 1: Weisungsberechtigte Person und Weisungsempfänger

Berechtigte Personen

Die nach § 6 Abs. (3) des Vertrages zur Weisung berechtigten Personen beim Verantwortlichen sind:

Vor- und Nachname	E-Mail-Adresse	Telefon

Notfallmanagement

Datenschutzrelevante Vorfälle gemäß § 5 Abs. (4) des Vertrages sind unmittelbar nach ihrer Feststellung und ohne schuldhafte Verzögerung vom Auftragnehmer an den Verantwortlichen zu melden. Hierfür sind auf Seiten des Verantwortlichen die folgenden Personen zu informieren:

Vor- und Nachname	E-Mail-Adresse	Telefon

Anlage 2: Technisch-organisatorische Maßnahme

§ 7 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Differenzierte Regelung der Benutzerberechtigungen und Verwaltung (Vergabe von Rechten, Entzug von Berechtigungen)
- Zwei-Faktor-Authentifizierung
- Vergabe von persönlichen Identifizierungsschlüsseln (SSH-Schlüssel)
- Personenbezogene Anmeldungen auf dem Server
- Einsatz von VPN-Technologie
- Automatische Updates der Sicherheitsrelevanten Anwendungen
- Beschränkung der öffentlichen Ports auf ein Minimum per Firewall

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Anzahl der Administratoren auf ein Minimum begrenzt
- Regelung von Zugriffsberechtigung in der Applikation
- Zugriff auf die Applikation nur nach vorheriger Authentifizierung
- Protokollierung von Eingaben/Veränderungen
- Datenzugriff nur durch Personen die im AV-Vertrag gelistet sind

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

-
- Sämtliche Daten verbleiben innerhalb des Datenverarbeitungssystems und werden nicht an Dritte weitergegeben
 - Verpflichtender Einsatz einer Transport-Verschlüsselung (TLS)
 - Sofortige Löschung aller Daten mit Ende des AV-Vertrags

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung von manuellen Eingaben/Veränderungen (Server-Log)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können:

- Automatische tägliche Sicherung des Gesamtsystems
- Automatische tägliche Sicherung der Datenbank
- Monitoring des Gesamtsystems

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

- Festlegung von Datenbankrechten
- Physische Trennung von Produktions- und Entwicklungssystemen
- Trennung zwischen der Verarbeitung von Produktions- und Testdaten