AUFTRAGSVERARBEITUNGSVERTRAG (AV-VERTRAG)

Stand 18. Juni 2025

zwischen

Schule (im Folgenden "Verantwortlicher")

Name der Schule: _____

Anschrift: _____

vertreten durch die Schulleitung: _____

und

app.schülerausweis.de
by Energy-Imaging: Die Experten für Schulmarketing
(im Folgenden "Auftragsverarbeiter")

Inhaberin Susanne Henkel
Schubertstraße 21, 40699 Erkrath
E-Mail: datenschutz@energy-imaging.de

---

1. Begriffsbestimmungen

Im Sinne dieses Vertrags gelten folgende Begriffsbestimmungen gemäß Art. 4 DSGVO:

- **Personenbezogene Daten:** Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
- **Verarbeitung:** Jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, Speichern, Ändern, Übermitteln oder Löschen.
- **Verantwortlicher:** Die Schule als datenverarbeitende Stelle, die über die Zwecke und Mittel der Verarbeitung entscheidet.
- **Auftragsverarbeiter:** app.schülerausweis.de by Energy-Imaging, das im Auftrag der Schule personenbezogene Daten verarbeitet.

---

2. Gegenstand und Dauer des Auftrags

2.1 Gegenstand der Verarbeitung

Der Auftragsverarbeiter stellt dem Verantwortlichen eine digitale Plattform zur Verfügung, um digitale Schüler- und Lehrerausweise zu generieren, zu speichern und zu verwalten. Hierbei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen.

Auf Wunsch des Verantwortlichen können zusätzliche Angaben auf dem Ausweis angezeigt werden, wie z. B. Barcodes für Bibliothek, Mensa oder Lehrmittelverwaltung. Ebenfalls kann die Adresse der Schüler*innen auf dem Ausweis dargestellt werden, sofern dies ausdrücklich von der Schule beauftragt wird. Der Auftragsverarbeiter empfiehlt dies jedoch aus Gründen der Datenminimierung ausdrücklich nicht, da der Ausweis primär zur Identifikation als Schüler*in sowie ggf. als Altersnachweis für Vergünstigungen dient.

2.2 Dauer des Vertrags

Dieser Vertrag tritt mit der Unterzeichnung in Kraft und bleibt gültig, solange der Verantwortliche die Dienste des Auftragsverarbeiters in Anspruch nimmt. Nach Beendigung des Vertrages endet die Auftragsverarbeitung automatisch. Eine gesonderte Kündigung dieses Vertrags ist nicht erforderlich. Nach Vertragsende werden die Daten gemäß Punkt 12 gelöscht.

---

3. Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt ausschließlich zum Zweck der Bereitstellung und Verwaltung digitaler Schüler- und Lehrerausweise. Dies umfasst:

- Erstellung und Speicherung von Ausweisen
- Verwaltung von Identifikationsdaten
- Integration in Apple Wallet, Google Wallet und PassWallet
- Authentifizierung und Sicherheit der Nutzerkonten
- Bereitstellung von Schnittstellen für Schulverwaltungen
- Technische Wartung und Support
- Schutz vor URL-Manipulation durch Verwendung signierter JSON Web Tokens (JWTs) zur Zugangskontrolle und Sitzungsverwaltung

---

4. Art der verarbeiteten personenbezogenen Daten

- Name, Vorname
- Geburtsdatum
- Schüler-ID aus der Schulverwaltung
- Foto
- E-Mail-Adresse

- Nutzungsdaten (IP-Adresse, Login-Zeiten, Gerätetyp)
- Optional: Barcode-IDs (z. B. für Bibliothek oder Mensa), Schüleradresse (nur wenn beauftragt)

Die Verarbeitung sensibler Daten gemäß Art. 9 DSGVO erfolgt nicht.

---

5. Pflichten des Verantwortlichen

Der Verantwortliche ist verpflichtet:

- Die Rechtmäßigkeit der Datenverarbeitung sicherzustellen (Art. 6 DSGVO)
- Betroffene Personen über die Verarbeitung zu informieren
- Die Weisungen an den Auftragsverarbeiter zu dokumentieren
- Sicherheits- und Datenschutzvorgaben innerhalb der Schule umzusetzen

---

6. Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich:

- Die Daten ausschließlich für die vereinbarten Zwecke zu verarbeiten
- Keine Daten an Dritte weiterzugeben, es sei denn, dies ist vertraglich geregelt
- Die Verarbeitung erfolgt grundsätzlich innerhalb der EU/des EWR. Eine Übermittlung in Drittstaaten erfolgt nur, sofern für das betreffende Drittland ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO besteht.
- Angemessene technische und organisatorische Sicherheitsmaßnahmen (TOMs) gemäß Art. 32 DSGVO zu implementieren.
- Schuladministratoren und betroffenen Personen den Zugang zu gespeicherten Daten zu ermöglichen
- Den Verantwortlichen unverzüglich zu informieren, wenn eine Weisung gegen Datenschutzrecht verstößt
- Den Verantwortlichen vor Verarbeitung zu informieren, wenn der Auftragsverarbeiter rechtlich zur anderweitigen Verarbeitung verpflichtet ist, sofern keine gesetzliche Geheimhaltungspflicht entgegensteht
- Sicherzustellen, dass sämtliche zur Verarbeitung personenbezogener Daten befugten Mitarbeitenden zur Vertraulichkeit verpflichtet sind. Alle Mitarbeitenden des Auftragsverarbeiters, die mit personenbezogenen Daten in Berührung kommen, unterzeichnen nach entsprechender Aufklärung eine Vertraulichkeits- und Verschwiegenheitserklärung
- Diese Verpflichtung zur Vertraulichkeit bezieht sich ausschließlich auf Mitarbeitende des Auftragsverarbeiters. Die Verpflichtung schulischer Mitarbeitender obliegt der verantwortlichen Stelle (Schule) gemäß Art. 32 Abs. 4 DSGVO

7. Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter hat folgende Maßnahmen zum Schutz personenbezogener Daten implementiert:

- **Zugriffsmanagement:**
  – Nutzer- und rollenbasierte Zugriffskontrollen
  – 2-Faktor-Authentifizierung für alle Administrations-Accounts
  – Passwortsicherheit nach aktuellen BSI-Empfehlungen
- **Transportverschlüsselung und Verfügbarkeit:**
  – TLS 1.2 oder höher für alle Datenübertragungen
  – Redundante Infrastruktur durch Hosting beim ISO 27001-zertifizierten Anbieter Mittwald in Deutschland
  – Tägliche Backups mit verschlüsselter Speicherung
- **Software-Sicherheit:**
  – Verwendung eines gehärteten TYPO3-CMS-Systems mit aktuellen Sicherheitsupdates
  – Regelmäßige Penetrationstests auf Anwendungsebene
  – Verhinderung unberechtigter Code-Ausführung über serverseitige Filter
- **Netzwerksicherheit:**
  – Firewall- und Intrusion-Detection-Systeme (IDS)
  – Überwachung aller Zugriffe auf Server und Plattformen (Logging & Monitoring)
- **Organisatorische Sicherheit:**
  – Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO
  – Mitarbeiterschulungen im Bereich Datenschutz und IT-Sicherheit
  – Internes Incident-Response-Management mit definierten Abläufen bei Datenschutzverstößen
- **Sicherung der Ausweisinhalte:**
  – Signierte JWTs zur Absicherung von URL-Zugriffen
  – Nutzer*innenspezifische Token mit Ablaufdatum zur Absicherung gegen Replay-Angriffe
  – Speicherung von Ausweisdaten verschlüsselt auf Servern und/oder Endgeräten (Apple Wallet, Google Wallet, PassWallet)

---

8. Unterauftragsverhältnisse

Die aktuell beauftragten Unterauftragsverarbeiter sind in **Anlage 1** aufgeführt. Eine Erweiterung oder Änderung erfolgt nur mit Zustimmung des Verantwortlichen.

---

9. Kontrollrechte der Schulen

Der Verantwortliche kann die Einhaltung dieses Vertrags überprüfen, z. B. durch:

- Einsicht in Protokolle
- Anforderung von Nachweisen
- Vor-Ort-Audit (nach Absprache)

---

10. Unterstützung bei Anfragen betroffener Personen

Anfragen betroffener Personen sind grundsätzlich durch den Verantwortlichen zu beantworten. Der Auftragsverarbeiter leitet ihm bekannte Anfragen unverzüglich weiter und unterstützt den Verantwortlichen bei der Bearbeitung. Die Unterstützung erfolgt so rechtzeitig, dass der Verantwortliche die Fristen gemäß Art. 12 Abs. 3 DSGVO einhalten kann (i. d. R. innerhalb von einem Monat nach Eingang der Anfrage)

---

11. Dokumentation der Weisungen des Verantwortlichen

Sämtliche Weisungen werden dokumentiert und auf Anfrage nachgewiesen.

---

12. Beendigung des Vertrags und Datenlöschung

Nach Vertragsende verpflichtet sich der Auftragsverarbeiter:

- Alle Daten zu löschen oder zurückzugeben
- Die Löschung auf Anfrage zu bestätigen
- Buchhaltungsdaten gemäß gesetzlichen Vorgaben aufzubewahren

---

13. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei:

- Datenschutz-Folgenabschätzungen (Art. 35 DSGVO)
- Konsultationen mit Datenschutzbehörden (Art. 36 DSGVO)
- Prüfungen durch Aufsichtsbehörden

Dieser AV-Vertrag ist Bestandteil der vertraglichen Vereinbarung zwischen Schule und Energy-Imaging. Änderungen bedürfen der Schriftform. Bei Widersprüchen zu anderen Vertragsdokumenten hat dieser AV-Vertrag Vorrang in datenschutzrechtlichen Fragen.

Unterschrift des Verantwortlichen (Schulleitung)	**Ort, Datum**
Unterschrift Auftragsverarbeiter	**Ort, Datum**

Anlage 1:
Liste der Unterauftragsverarbeiter

Unternehmen	Aufgabe	Ort der Verarbeitung
Mittwald	Hosting & Server	Deutschland / EU
IONOS (1&1)	Hosting von Matomo (selbstgehostet)	Deutschland / EU
Brevo	E-Mail-Versand	EU
Apple	Anzeige und Verwaltung digitaler Ausweise über Apple Wallet. Speicherung und Anzeige des Schülerausweises auf dem Endgerät; keine Datenverarbeitung durch Apple im Auftrag	lokal auf Endgeräten, nutzerabhängig
PassWallet	Anzeige und Verwaltung von Ausweisen auf Android-Geräten. Lokale Anzeige von Ausweisdaten auf Android-Geräten; keine Datenverarbeitung durch PassWallet im Auftrag	lokal auf Endgeräten, nutzerabhängig
Google Wallet API	Bereitstellung digitaler Ausweise über Google Wallet. Speicherung des Schülerausweises auf Android-Geräten; API-Nutzung zur Integration; Google verarbeitet technische Metadaten zur Bereitstellung des Dienstes	Google-Infrastruktur (DSGVO/GDPR-Garantien von Google)
WebUntis	Schnittstelle zur Schulverwaltung (optional)	Österreich / Deutschland
HubSpot	Support & CRM (bei Bedarf)	Deutschland
Vidyard	Bereitstellung von Video-Content (z. B. Tutorials, Erklärvideos) für Schuladministration oder Schüler*innen. Technische Bereitstellung und Streaming von vorab hochgeladenen Videos. IP-Adresse und Gerätedaten der Zuschauenden werden beim Abruf verarbeitet. Keine Auswertung im Auftrag.	Kanada (mit Angemessenheitsbeschluss)
United Domains	Domainverwaltung & SSL-Zertifikate. Verwaltung der schulbezogenen Subdomains (z. B. schule.app.schuelerausweis.de), Bereitstellung von HTTPS-Zertifikaten	Deutschland
Stripe	Zahlungsdienstleister (bei Bedarf)	EU