

**Dieser Vertrag dient zur Ansicht!
Bei Kauf des Portfolio-Pakets und/oder
Support-Abos wird er mit angepasster Ad-
resse, Vertragsnummer und Datum an Ihre
Schule geschickt.**

Lena Widmann
Amalienstraße 53
76133 Karlsruhe
widmann.lena@gmail.com
www.lenawidmann.de

Vertrag

Nr. 2018-0000-0000 | 00.00.2018

über eine Auftragsdatenverarbeitung nach Art. 28 der
Europäischen Datenschutz-Grundverordnung (EU-DSGVO)

Zwischen

Name der Schule

- nachfolgend „Auftraggeber“ genannt - und

Lena Widmann

- nachfolgend „Auftragsverarbeiter“ genannt -
wird folgender Vertrag geschlossen:

§ 1 Gegenstand, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen (Auftrag)

Der Auftraggeber nutzt die vom Auftragsverarbeiter angebotenen IT-Services zur Durchführung der folgen-
den Auftragsdatenverarbeitung:

- Erstellung, Wartung und Aktualisierung des Online-Schulportfolios von /// plattformblatt, das gestalterisch
individuell an die Schule angepasst wird

Die Verarbeitung erfolgt auf folgende Art (Verarbeitungsweise) und zu folgendem Zweck:

- Anpassen des Impressums des Online-Portfolios als grundlegender Inhalt des Web-Auftritts
- erstes Anlegen von Benutzern und deren Nutzungsrechten im Online-Portfolio als Zugang zum
geschützten Bereich (auf dem Testserver von /// plattformblatt und später auf dem Server der Schule)
- Übertragung des Portfolio-Pakets mit Datenbank auf den Server der Schule zur Installation
- Unterstützung bei der Installation des Portfolio-Pakets und der Datenbank (nach Absprache)
- ständige technische Wartung und Aktualisierung des Online-Portfolios zur Sicherheit der Plattform
- die Schule abonniert den Support-Newsletters, um über die aktuellen Änderungen informiert zu werden

Dabei werden die in Anlage 2 beschriebenen personenbezogenen Daten von folgenden betroffenen Personen
verarbeitet: Schulleitung, Lehrer*innen aus dem Portfolio-Team, Datenschutzbeauftragte*r.

Es gelten die Begriffsbestimmungen gemäß EU-DSGVO.

§ 2 Dauer der Verarbeitung

Die Verarbeitung beginnt mit dem Zeitpunkt der Bereitstellung der Daten zur Erstellung des Online-Portfolios für die Schule und endet mit der Kündigung des Support-Abos.

Eine Vertragspartei kann jeweils mit einer Frist von zwei Wochen zum Monatsende kündigen.

Darüber hinaus können die Vertragspartner den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß einer Vertragspartei vorliegt (außerordentliche Kündigung).

§ 3 Anwendungsbereich

3.1 Der Umfang der Datenverarbeitung, die erfassten Zugangsdaten (z. B. Account) sowie die Datenarten, die im Rahmen der Nutzung verarbeitet werden, entstehen (z. B. Log-Daten) bzw. entstehen können, werden in der Anlage 2 dokumentiert.

3.2 Betroffen von dieser Datenverarbeitung ist der unter Nr. 1 dieses Vertrages aufgeführte Personenkreis.

3.3 Umfang des Vertrags

Der Auftragverarbeiter erstellt das Portfolio-Paket mit „Joomla!“ und verschiedenen Joomla-Erweiterungen. Joomla ist ein freies Content-Management-System zur Erstellung von Webseiten. Die Website des Portfolio-Pakets ist so gestaltet, dass sie der Schule als Plattform zur Dokumentation und Präsentation des Schulportfolios dient. Sie wird der Schule leer bzw. mit Beispieldaten zur Verfügung gestellt, so dass sie mit eigenen Inhalten gefüllt werden kann. Für die Inhalte ist die Schule selbst verantwortlich.

Die Plattform enthält ein dreispaltiges Menü mit veränder- und erweiterbaren Gliederungspunkten, die eine einfache Zuordnung der schulischen Dokumente ermöglichen. Beispieldaten und Vorlagen erleichtern die Erstellung und Bearbeitung der Dokumente in Zusammenhang mit der Präsentation des Schulportfolios. Mit der durchgängigen Gestaltung wird Kontinuität gewahrt.

Übersichtlichkeit und einfaches Handling zeichnen auch den Bearbeitungsbereich mit aus. Ausgewählte Personen können sich über die Plattform anmelden und zeit- und ortsunabhängig direkt im Browser über eine einfache Benutzeroberfläche am Portfolio arbeiten. Standard sind außerdem eine plattforminterne Suche, ein Kalender mit Kategorien sowie eine Druck- und Download-Funktion.

Das Aussehen der Plattform wird durch die Verwendung des Schullogos und gegebenenfalls weiterer charakteristischer Elemente an die Schule angepasst.

Der Auftragsverarbeiter stellt für die Erstellung und das Testen des individuell angepassten Online-Portfolios die notwendigen Server sowie die notwendige Infrastruktur bereit. Während der Anpassungen an die Schule wird die Plattform einem Ansprechpartner über einen Testserver zugänglich gemacht.

Wenn nicht anders vereinbart, wird ein Web-Hosting Anbieter von der Schule gewählt und beauftragt. Die Plattform basiert auf dem Content Management System Joomla. Dafür wird mindestens PHP 7 und eine MySQL Datenbank benötigt. Außerdem ist das Reservieren einer Domain erforderlich. Es kann auch eine Subdomain zur Schulwebsite (falls vorhanden) erstellt werden. Für die Datenübertragung, Installation (nach Absprache), Wartung und Aktualisierung stellt der Auftraggeber die notwendigen Server sowie die notwendige Infrastruktur bereit und ermöglicht dem Auftragsverarbeiter dauerhaften Zugang.

Der Auftragsverarbeiter wird die vollständige Website mit der Portfolio-Plattform verpackt zusammen mit einer Datenbank-Datei per FTP (File Transfer Protocol) auf den Server der Schule laden. Wenn nicht anders vereinbart wird die Installation durch den Systemadministrator der Schule durchgeführt.

Mit dem Support-Abo übernimmt der Auftragsverarbeiter die regelmäßige technische Wartung, die Durchführung aktueller Sicherheitsupdates und die Aktualisierung der Plattform mit neuen Features. Für die Wartung werden vor allem zwei Erweiterungen genutzt: Watchful und Akeeba Backup.

Die Joomla!-Erweiterung „Watchful“ ermöglicht dem Auftragsverarbeiter die automatische Prüfung auf Updates auf der Plattform der Schule und deren Aktualisierung über einen Account auf watchful.li ohne separate Anmeldung im Joomla!-Backend des Schulportfolios.

„Akeeba Backup“ ist eine Komponente zum sichern der Joomla-Installation. Dabei wird die Datenbank mit den Inhalten ebenso gesichert wie die FTP-Daten mit der Struktur der Website. Das Backup wird auf dem Server innerhalb der Website-Struktur gespeichert, kann aber auch heruntergeladen und an anderer Stelle gespeichert werden. Akeeba Backup enthält ein Installationscript, das die Joomla-Installation bei Bedarf wieder herstellt.

Die Server des Auftragsverarbeiters werden regelmäßig gesichert. Der Auftragsverarbeiter richtet mit dem Support-Abo eine Hotline für technische Probleme ein.

Einzelheiten zu den genutzten Diensten werden stets aktuell auf der Homepage www.plattformblatt.de des Auftragsverarbeiters beschrieben.

§ 4 Verantwortung für personenbezogene Daten

4.1 Damit diese Dienste genutzt werden können, müssen die oben beschriebenen Datenarten auf den Servern des Auftragsverarbeiters verarbeitet werden. Außerdem benötigt der Auftragsverarbeiter Zugang zu den Servern des Auftraggebers. Der Auftraggeber ist verantwortlich für die Daten im Sinne des Datenschutzrechts (Art. 4 Nr. 7 EU-DSGVO). Um dieser Verantwortung gerecht zu werden, enthält dieser Vertrag eine detaillierte Darstellung der Datenverarbeitungspflichten des Auftragsverarbeiters sowie der Rechte und Pflichten des Auftraggebers. Diese sind in der Anlage 1 des Vertrages ausführlich dargestellt.

4.2 Der Auftragsverarbeiter hat umfangreiche technische und organisatorische Maßnahmen zu ergreifen und aufrecht zu erhalten, um die Daten vor dem Zugriff Dritter oder Datenverlust zu schützen. Die Maßnahmen ergeben sich aus der Anlage 2.

§ 5 Pflichten und Rechte der Vertragsparteien

5.1 Auftragsverarbeiter

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

5.2 Im Übrigen ergeben sich die Rechte und Pflichten der Vertragsparteien aus der Anlage 1.

§ 6 Sonstiges

Änderungen oder Ergänzungen dieses Vertrages bedürfen nach Art 28 Abs. 9 EU-DSGVO der Schriftform. Gleiches gilt für die Aufhebung des Schriftformerfordernisses selbst.

Sollte eine Regelung dieses Vertrages nichtig sein oder werden oder sich eine Lücke herausstellen, bleibt der Vertrag im Übrigen gültig. Es soll das gelten, was die Parteien vereinbart hätten, wenn die Unwirksamkeit oder die Lücke bekannt gewesen wäre.

Die Vertragsparteien prüfen dann gemeinsam, ob Änderungen oder Ergänzungen dieses Vertrages erforderlich sind. Kommen sie zu dem Ergebnis, dass eine Änderung oder Ergänzung des Vertrages erforderlich ist, oder wird von einer Vertragspartei eine Änderung oder Ergänzung dieses Vertrages beantragt, so nehmen sie unverzüglich Verhandlungen auf.

Anlage 1

„Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsdatenverarbeitung“
und

Anlage 2

„Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen“
sind Bestandteil dieses Vertrages.

Ort, Datum

Ort, Datum

Auftraggeber

Auftragsverarbeiter

Anlage 1

Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsdatenverarbeitung zum Vertrag über eine Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO

Name der Schule

- nachfolgend „Auftraggeber“ genannt - und

Lena Widmann

- nachfolgend „Auftragsverarbeiter“ genannt.

§ 1 Pflichten des Auftragsverarbeiters

1.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle nach Art. 32 EU-DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Art. 32 Abs. 1 EU-DSGVO regelt hierzu:

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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

- a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
- b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
- c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
- d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen so gesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.2 Der Auftragsverarbeiter stellt dem Auftraggeber zu Beginn dieses Vertrages in Anlage 2 ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung. Dieses Konzept beschreibt nach Art. 32 Abs. 2 EU-DSGVO 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 die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner sind die Voreinstellungen darzustellen, die u. a. gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

Änderungen in diesem Konzept sind dem Auftraggeber vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagieren zu können. Die jeweils aktuelle Fassung des Konzepts wird dem Auftraggeber zur Kenntnisnahme und Zustimmung mindestens vier Wochen vor Umsetzung des Konzepts übersandt.

1.3. Der Auftragsverarbeiter stellt dem Auftraggeber die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO programm- bzw. verarbeitungsspezifischen notwendigen Angaben zur Verfügung (Anlage 2). Der Auftraggeber sollte in seinem Verzeichnis der Verarbeitungstätigkeiten auf das gesamte Vertragswerk zur Auftragsdatenverarbeitung verweisen. Ferner führt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag der Auftraggebers durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 EU-DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.4 Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

1.5. Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten des betrieblichen oder behördlichen Datenschutzbeauftragten mit.

1.6. Der Auftragsverarbeiter unterrichtet die Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs.2 EU-DSGVO).

1.7. Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle 5 Jahre.

1.8. Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Die Verarbeitung der Daten in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum bedarf der vorherigen Zustimmung des Auftraggebers.

1.9 Nach Ende der Verarbeitung muss der Auftragsverarbeiter nach Wahl des Auftraggebers diesem alle personenbezogene Daten entweder zurückgeben oder spätestens innerhalb eines Monats löschen. Sofern die personenbezogenen Daten zurückgegeben werden, muss der Auftragsverarbeiter diese anschließend bei sich löschen. Der Auftragsverarbeiter hat dem Auftraggeber die Löschung umgehend schriftlich zu bestätigen. Die Bestimmungen des Landesarchivgesetzes sind zu beachten.

§ 2 Pflichten des Auftraggebers

2.1. Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der IT-Services Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2.2. Der Auftraggeber, als für den Datenschutz Verantwortlicher, ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO zuständig.

2.3. Dem Auftraggeber obliegt die Einhaltung der in den Artikeln 32 bis 36 EU-DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen.

Ferner obliegen dem Auftraggeber die aus den Artikeln 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

§ 3 Kontrollmaßnahmen und Weisungsbefugnis

Der Auftraggeber überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Auftraggeber oder dessen Beauftragter kann sich hierüber auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Auftraggeber oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragsverarbeiters ein.

Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der EU-DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder ein genehmigtes Zertifizierungsverfahrens gemäß Artikel 42 EU-DSGVI durch den Auftragsverarbeiter eingehalten werden, erbringen.

Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der

Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellen sowie Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die EU-DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Der Auftraggeber hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter erteilt dem Auftraggeber die hierfür notwendigen Auskünfte und ermöglicht die Überprüfung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen in geeigneter Weise. Im Falle einer Überprüfung durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gilt dies entsprechend. Der Auftragsverarbeiter gestattet dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß Art. 58 Abs. 1 lit. e EU-DSGVO jederzeit Zutritt zu den Räumen, in denen er Daten des Auftraggebers im Auftrag verarbeitet, und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung dessen Aufgaben notwendig sind.

§ 4 Unterauftragsverhältnisse

4.1. Dem Auftragsverarbeiter wird allgemein gestattet, Subunternehmer als Unterauftragnehmer in Anspruch zu nehmen. Der Auftragsverarbeiter muss dies gegenüber dem Auftraggeber innerhalb von vier Wochen vor Beginn der Verarbeitung durch einen Subunternehmer schriftlich anzeigen. Der Auftraggeber kann dagegen Einspruch erheben. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

4.2. Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 EU-DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

4.3. Der Auftragsverarbeiter verwendet für die Datenspeicherung Server in seinem Rechenzentrum. Die Kundenbetreuung und die technische Betreuung erfolgt direkt über den Auftragsverarbeiter.

§ 5 Informationspflicht

Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auf-

tragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der EU-DSGVO liegen.

§ 6 Sonstiges

Die Vertragspartner vereinbaren, die datenschutzrechtlichen Bestimmungen einzuhalten und ihre Mitarbeiterinnen und Mitarbeiter hierzu zu verpflichten.

Anlage 2

Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen

DATENSCHUTZ

§ 1 Umfang der Datenverarbeitung, erfasste Zugangsdaten und Datenarten, die im Rahmen der Nutzung verarbeitet werden, entstehen bzw. entstehen können.

Vertragsdaten

Der Auftragsverarbeiter erhebt, verarbeitet und speichert die Daten, die Sie angeben, wenn Sie bei /// plattformblatt bestellen. Außerdem speichert und verarbeitet der Auftragsverarbeiter Daten über den Auftrags- und Zahlungsverlauf.

Kontakt Daten

In der Kundendatenbank speichert der Auftragsverarbeiter Kontaktdaten der Ansprechpartner in der Schule.

Die individuell an die Schule angepasste Portfolio-Plattform enthält wie jede Website ein Impressum. Dieses Impressum wird vom Auftragsverarbeiter mit Name, E-Mail-Adresse, Telefonnummer und Adresse der Schule bzw. der Schulleitung und des Datenschutzbeauftragten ergänzt. Diese Daten werden dafür vom Auftraggeber zur Verfügung gestellt.

Zugangsdaten

Der Auftraggeber bekommt einen Account zur individuell an die Schule angepassten Testversion des Portfolios auf dem Server des Auftragverarbeiters. Das Anlegen von Benutzern und Nutzungsrechten benötigt Name, Benutzername und E-Mail-Adresse von der Schulleitung und den Lehrkräften aus dem Portfolio-Team. Nach der Übertragung des gesamten Portfolios auf den Server der Schule können die Zugangsdaten der Benutzer vom Administrator des Schulportfolios selbst geändert werden.

Mit dem Support-Abo bleibt der Account des Auftragsverarbeiters zum Portfolio der Schule auch nach der Übertragung bestehen. Das heißt, der Auftragsverarbeiter bekommt dauerhaften Backend-Zugriff als Super User bzw. Administrator, um technische Wartungsarbeiten und die Aktualisierung oder Neugestaltung von Features durchführen zu können.

Der Auftraggeber erhält einen Account für den Supportbereich von ///plattformblatt. Der Auftragsverarbeiter erstellt einen Account für die Schule und gibt die Zugangsdaten telefonisch durch. Die sichere Aufbewahrung und Handhabung liegt in der Verantwortung des Auftraggebers.

Der Auftragsverarbeiter bekommt vom Auftraggeber einen FTP-Zugang zum Server der Schule: Servername, FTP-Benutzername und Passwort. Der Zugang kann auf den Bereich begrenzt sein, auf dem die Website-Daten des Portfolios liegen. Der Zugang wird vom Auftragsverarbeiter zur Datei- und Datenbank-Übertragung des Portfolios benötigt.

Mit dem Support-Abo wird dem Auftragsverarbeiter der dauerhafte Zugang via FTP ermöglicht, um regelmäßige Wartungsarbeiten durchführen zu können.

Nach Absprache kann der Auftragsverarbeiter den Auftraggeber bei der Installation des Portfolios auf dem eigenen Server unterstützen. Dazu benötigt der Auftragsverarbeiter die Zugangsdaten zum Kundenbereich des Webhosting-Anbieters der Schule, um die Datenbank zu installieren und die configuration.php der Joomla-Installation mit den Server-Daten anzupassen.

Daten im Rahmen der Nutzung von Testversion, Demo-Version und Supportbereich

Die Webseiten des Auftragsverarbeiters werden bei Strato gehostet. Die an die Schule angepasste Testversion des Portfolios wird über einer Subdomain zu plattformblatt.de zugänglich gemacht. Somit verarbeitet Strato Daten der Testversion, die auf den Strato-Servern gespeichert werden. Dies umfasst die Herstellung von Sicherheitskopien in den Backup-Systemen von Strato.

Nach der Übertragung der Website-Daten und Datenbank auf den Server der Schule wird die Installation auf dem Strato-Server gelöscht.

Der Versand des Support-Newsletters erfolgt mittels des Versanddienstleisters „MailChimp“, einer Newsletterversandplattform des US-Anbieters Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, USA. Die Datenschutzbestimmungen des Versanddienstleisters können Sie hier einsehen: <https://mailchimp.com/legal/privacy/>. The Rocket Science Group LLC d/b/a MailChimp ist unter dem Privacy-Shield-Abkommen zertifiziert und bietet hierdurch eine Garantie, das europäische Datenschutzniveau einzuhalten (<https://www.privacyshield.gov/participant?id=a2zt0000000TO6hAAG&status=Active>). Der Versanddienstleister wird auf Grundlage berechtigter Interessen gem. Art. 6 Abs. 1 lit. f. DSGVO und eines Auftragsverarbeitungsvertrages gem. Art. 28 Abs. 3 S. 1 DSGVO eingesetzt.

Der Versanddienstleister kann die Daten der Empfänger in pseudonymer Form, d.h. ohne Zuordnung zu einem Nutzer, zur Optimierung oder Verbesserung der eigenen Services nutzen, z.B. zur technischen Optimierung des Versandes und der Darstellung der Newsletter oder für statistische Zwecke verwenden. Der Versanddienstleister nutzt die Daten unserer Newsletterempfänger jedoch nicht, um diese selbst anzuschreiben oder um die Daten an Dritte weiterzugeben.

Log-Daten bei Strato

Wenn Sie die Webseiten von /// plattformblatt besuchen oder unsere Dienste nutzen übermittelt das Gerät, mit dem Sie die Seite aufrufen, automatisch Log-Daten (Verbindungsdaten) an die Server von Strato. Log-Daten enthalten die IP-Adresse des Gerätes, mit dem Sie auf die Website oder einen Dienst zugreifen, die Art des Browsers, mit dem Sie zugreifen, die Webseite, die Sie zuvor besucht haben, Ihre Systemkonfiguration sowie Datum und Zeitangaben. Strato speichert IP-Adressen nur, soweit es zur Erbringung der Dienste erforderlich ist. Ansonsten werden die IP-Adressen gelöscht oder anonymisiert. Die IP-Adressen speichert Strato zur Erkennung und Abwehr von Angriffen maximal 7 Tage.

Mehr Informationen dazu finden Sie unter <https://www.strato.de/datenschutz/> und <https://strato.de/blog/dsgvo-logfiles/>

www.plattformblatt.de

Die Datenschutzerklärung zum Online-Angebot von /// plattformblatt können Sie jederzeit unter diesem Link einsehen: <https://plattformblatt.de/Datenschutzerklaerung/>

SICHERHEITSKONZEPT

§ 1 Daten auf dem Server des Auftragsverarbeiters

Der Auftragsverarbeiter nutzt Server des Webhosting-Anbieters Strato: www.strato.de.

Das Sicherheitskonzept von Strato ist über diesen Link einzusehen: <https://www.strato.de/sicherheit/>

Strato unterhält zertifizierte Rechenzentren. Alle Server stehen in Deutschland.

Der Zugriff des Auftragsverarbeiters auf den eigenen Server bei Strato erfolgt per Secure Shell (SSH). SSH ist ein Netzwerkprotokoll, das eine verschlüsselte Netzwerkverbindung mit einem entfernten Gerät herstellt. Die Datenübertragung auf den Server erfolgt somit per SFTP (SSH File Transfer Protocol oder Secure File Transfer Protocol).

Der Auftragsverarbeiter erstellt das an die Schule angepasste Portfolio zunächst auf dem eigenen Server (gehostet bei Strato). Es steht der Schule dort vor der Übergabe und Installation auf dem Schulserver zum Testen zur Verfügung. Dazu bekommt die Schule Zugangsdaten vom Auftragsverarbeiter. Die Testversion ist über eine Subdomain von plattformblatt.de per HTTPS zugänglich. HTTPS (Hypertext Transfer Protocol Secure) ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen. Es stellt eine Transportverschlüsselung dar. Alle Seiten von [/// plattformblatt](http://plattformblatt.de), z.B. der Supportbereich und die Demo-Version sind per HTTPS zugänglich.

§ 2 Daten auf den Servern des Auftraggebers

Nach der Übertragung der Daten auf den Server des Auftraggebers ist der Auftraggeber bzw. dessen Webhost (z.B. [belwü](http://belwu.de)) selbst für die Sicherheit der Daten und der Datenübertragung verantwortlich.

§ 3 Datenaustausch zwischen Auftraggeber und Auftragsverarbeiter

Der Austausch von Zugangsdaten – zum Server, zum Joomla-Backend, zum Supportbereich und ggf. zum Kundenaccount des Webhosting-Anbieters der Schule – erfolgt ausschließlich telefonisch. Der Auftragsverarbeiter speichert diese Daten auf dem passwortgeschützten PC in einem verschlüsselten passwortgeschützten Ordner (siehe Speicherung der Kundendaten beim Auftragsverarbeiter).

Der Auftraggeber ist für die Verschlüsselung und passwortgeschützte Speicherung auf dem eigenen System selbst verantwortlich. Die vom Auftragsverarbeiter angelegten Benutzer können und sollten ihre Zugangsdaten nach der Übergabe des Portfolio-Pakets von ihrem Portfolio-Administrator ändern lassen.

Die FTP-Daten und die Datenbank des Portfolio-Pakets werden vom Auftragsverarbeiter per FTP (File Transfer Protocol) auf den Server der Schule geladen. Der Auftragsverarbeiter verwendet dafür die vom Auftraggeber bereitgestellte Übertragungsart. Bestenfalls wird für den Auftraggeber eine SSH-verschlüsselte Netzwerkverbindung eingerichtet.

§ 4 Speicherung von Kundendaten beim Auftragsverarbeiter

Der Auftragsverarbeiter speichert die Kundendaten in einem verschlüsselten und passwortgeschützten Ordner auf einem passwortgeschützten PC und einer externen Festplatte mit automatisch erstellten Backups.

Die Verschlüsselung ist eine 256-Bit-AES-Verschlüsselung. Der Advanced Encryption Standard (AES) ist ein symmetrisches Verschlüsselungsverfahren, bei dem ein Klartextabschnitt fester Länge, auf einen Geheim-

oder Schlüsseltextblock fester Länge abgebildet wird. Diese Abbildung wird dabei durch einen Schlüssel beeinflusst. Kennt man diesen, kann man aus dem Geheimtext wieder den Klartext berechnen. Ohne Kenntnis des Schlüssels ist dies hingegen praktisch unmöglich. Die 256-Bit-AES-Verschlüsselung bietet ein sehr hohes Maß an Sicherheit.

Das Passwort entspricht in Länge und Zeichenwahl den aktuellen Sicherheitsempfehlungen und wird nirgends als Klartext gespeichert oder notiert.