Datenschutzrechtliche Erklärung

zwischen dem

Förderverein Bayerisches Realschulnetz e.V.
c/o Wilhelm-Leibl-Realschule Bad Aibling
z.Hd. Vorsitzender Matthias Wabner
Max-Mannheimer-Str. 1
83043 Bad Aibling

im nachfolgenden „Auftragnehmer“ genannt und

Schule /Institution	
Schulname:	
Schulnummer:	
Straße, Nr.:	
PLZ:	
Ort:	
E-Mail-Adresse:	

im nachfolgenden „Auftraggeber“ genannt.

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäfts- und Behördengeheimnissen des Auftraggebers vertraulich zu behandeln. Der Auftragnehmer hat grundsätzlich alle seine Mitarbeiter, denen im Rahmen des Vertragsverhältnisses Daten des Auftraggebers bekannt werden, verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Daten, soweit sie nicht offenkundig sind, nicht an Dritte weiterzugeben. Grundsätzlich hat der Auftraggeber Weisungsbefugnis an den Auftragnehmer in allen datenschutzrelevanten Sachverhalten sowie das Recht einer Überprüfung der Einhaltung der Datenschutzmaßnahmen des Auftragnehmers. Dies gilt ebenfalls für die Daten, auf die der Auftragnehmer z.B. für Programmierung und/oder für die Störungsbeseitigung zugreifen muss sowie Daten, die nach Freigabe des Auftraggebers, für eine weitere Bearbeitung auf einem Simultansystem zwischengespeichert werden sollen. Die Bereitstellung solcher Daten auf einem Simultansystem

stellt keine Übermittlung im datenschutzrechtlichen Sinne dar. Der Auftragnehmer verpflichtet sich, die Daten nach Beendigung der Arbeiten auf dem Simultansystem ohne besondere Aufforderung datenschutzgerecht zu löschen und nicht an Dritte weiterzugeben. Bei vereinbarter Vernichtung der Daten inkl. aller auch vom Auftragnehmer erstellten Kopien (auch Datensicherungen), ist diese unaufgefordert und unverzüglich nach Beendigung der Arbeiten durchzuführen und seitens des Auftragnehmers gegenüber dem Auftraggeber zu erklären, dass sämtliche Daten oder Kopien (auch Datensicherungen) vernichtet oder zurückgegeben sind. Der Auftragnehmer greift im Sinne der Datenvermeidung und der Datensparsamkeit ausschließlich nur auf solche personenbezogenen Daten zu, die für die Zweckerfüllung (Zweckbindung der Daten) des jeweiligen Auftrages unbedingt erforderlich (Erforderlichkeit) sind. Von dieser Erklärung unberührt besteht das Recht des Auftraggebers auf Schadensersatz, Wandlung des Auftrages, Rückforderung bereits geleisteter Zahlungen, sofern im Sinne dieser Vereinbarung der Auftragnehmer seine Pflichten, wissentlich oder grob fahrlässig nicht erfüllt. Von dieser Erklärung unberührt bleibt die Verpflichtung des Auftraggebers, seine Daten vor dem Zugriff Dritter zu schützen und zu sichern. Im Besonderen finden die Regelungen des Datenschutzgesetzes Anwendung und sind Bestandteil dieser Erklärung. Technische und organisatorische Maßnahmen bei Auftragsdatenverarbeitung gemäß §§ 9, 11 Abs. 3 Nr. 3 Bundesdatenschutzgesetz (BDSG) Die Daten werden im Rechenzentrum der Hetzner Online AG in Nürnberg verarbeitet. Folgende Sicherungsmaßnahmen sind getroffen: Zutrittskontrolle: Der Zutritt in das Gebäude wird durch Identifikation mit einem RFID Schlüssel und Rackschlüssel geregelt. Jeder Zutritt wird mit Bild, Zugangs- und Abgangszeit sowie Datum protokolliert. Zutritt zum Rechenzentrum erhalten ausschließlich nur Mitarbeiter, die zur Ausübung ihrer Tätigkeit den Zutritt benötigen. Angelegt und authorisiert werden die Zutritte durch den Vereinsvorsitzenden. Der RFID Schlüssel als auch der Rackschlüssel wurden jeweils gegen Unterschrift und Vorlage eines Personalausweises von Hetzner Online AG an vom Vereinsvorsitzenden bestimmte Mitarbeiter des Vereins ausgegeben. Dieser ist derzeit nur zwei Mitarbeitern des Fördervereins Bayerisches Realschulnetz gestattet. Weitere Berechtigungen werden ausschließlich nach Rücksprache mit und mit Genehmigung des Vereinsvorsitzenden erteilt. Zugangskontrolle: Der Zugang zu Systemen erfolgt über Login-Name und Passwort . Einen Login zu den entsprechenden Systemen erhalten nur Mitarbeiter, die zur Ausübung Ihrer Tätigkeit diesen Zugang benötigen. Die Zugänge werden schriftlich beantragt und durch die verantwortliche Person für dieses System genehmigt. Erteilt werden die Zugänge durch den technischen Leiter. Es finden regelmäßige Prüfungen statt, bei der die vorhandenen Zugänge eines jeden Mitarbeiters auf Notwendigkeit überprüft werden. Wenn ein Mitarbeiter einen bestimmten Zugang zur Ausübung seiner Tätigkeit nicht mehr benötigt, werden die entsprechenden Zugänge deaktiviert. Zugriffskontrolle: Die Zugriffskontrolle erfolgt durch spezielle Passwörter und Berechtigungen, die individuell vergeben werden. Zugriff erhalten nur Mitarbeiter, die zur Ausübung Ihrer Tätigkeit diesen entsprechenden Zugriff auch benötigen Antrags- und Prüfungsverfahren wie unter Zugangskontrolle beschrieben. Weitergabekontrolle: Die Weitergabe der Daten wird durch die Protokollierung der Datenverarbeitung gewährleistet. Des Weiteren werden die Daten mit einer verschlüsselten Datenübertragung gesichert. Eingabekontrolle: Eine Eingabe kann nur durch die Mitarbeiter erfolgen, die Zugriff auf die Daten haben (siehe Zugangskontrolle). Je nach Funktion des Mitarbeiters werden die Zugriffe differenziert vergeben (z.B. nur Leserechte usw.). Eingeben, Verändern und Entfernen wird automatisch für

bestimmte Aktionen am System protokolliert und kann im Einzelfall nachvollzogen werden. Auftragskontrolle: Die Auftragskontrolle ist durch die automatischen Prozesse gewährleistet. Alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind auf das Datengeheimnis nach §5 BDSG verpflichtet. Änderungen und Neuerungen werden den Mitarbeitern in geeigneter Form mitgeteilt. Verfügbarkeitskontrolle: Die Verfügbarkeitskontrolle wird durch regelmäßige Datensicherung und Backups der entsprechenden Datenbanken und Systeme gewährleistet. Für den Fall eines Stromausfalls besteht eine redundante Stromversorgung und Kühlung. Zum Schutz der Systeme existieren Firewalls, regelmäßige System- Updates, skalierbare USV- und Kühlsysteme, mehrfache Hochgeschwindigkeitsanbindung des Backbones und weitere Schutzmaßnahmen wie etwa Virenscanner. Trennungsgebot: Alle gelieferten Datenpakete werden voneinander getrennt bearbeitet, so dass eine Überschneidung von Schuldaten ausgeschlossen ist. Hierzu sind entsprechende technische Vorkehrungen getroffen.

Schulstempel

Auftraggeber	**Auftragnehmer**
Ort, Datum, rechtsverbindliche Unterschrift	Ort, Datum, rechtsverbindliche Unterschrift