ANHANG 3 *zum Leitfaden «Datensicherheit für Lehrpersonen und Schulleitungen»*
Hrsg.: VBE, GÖD, LCH 2015.
Bezug: www.medien-datensicherheit-schulen.info
Alle Links sind aktiv geschaltet.

MUSTER FÜR EINEN AUFTRAGSDATENVERTRAG (DEUTSCHLAND, NRW)

Vertrag über eine Auftragsdatenverarbeitung
gemäß § 11 DSG NRW Vereinbarung
zwischen der
xyz Schule, ABC Straße, Musterhausen

– nachstehend Auftraggeber genannt –
und dem/der

– nachstehend Auftragnehmer genannt –

1. GEGENSTAND UND DAUER DES AUFTRAGS

Gegenstand des Auftrags

Gegenstand des Auftrags ist die Durchführung folgender Tätigkeiten bzw. Erbringung folgender Leistungen durch den Auftragnehmer:

- Webservices
- allg. Supportdienstleistungen
- Hostingdienstleistungen
- Softwareservicedienstleistungen

Dauer des Auftrags

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von drei Monaten zum Quartalsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. KONKRETISIERUNG DES AUFTRAGSINHALTS

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Der Zweck und Umfang der Auftragsdatenverarbeitung ist:

- Betrieb und Pflege der Webseite
- Betreuung und Support der Computersysteme im Verwaltungs- und Schulbereich
- Betreuung der technischen Infrastruktur
- Betrieb und Support der xyz Anwendung
- ...

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen des § 17 DSG NRW erfüllt sind.

Art der Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- Name
- Adresse
- Geburtsdatum
- Telefon
- Benotung
- Gesundheitsinformationen

Kreis der Betroffenen
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung/Beschreibung der betroffenen Personenkategorien):

- Schüler/inne
- Ehemalige Schüler/innen
- Lehrer/innen
- Ehemalige Lehrer/innen
- Eltern
- ...

3. TECHNISCH-ORGANISATORISCHE MASSNAHMEN

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und des Trennungsgebots (vgl. auch Anlage § 11 BDSG) sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs/der Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand, die – soweit sie sich nicht aus der zugrunde liegenden Leistungsvereinbarung ergeben – im Anhang detailliert aufgeführt sind.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG bzw. § 32a Abs. 3 DSD NRW dem Auftraggeber zur Verfügung zu stellen.

4. BERICHTIGUNG, SPERRUNG UND LÖSCHUNG VON DATEN

Der Auftragnehmer hat keinerlei Berechtigung, Daten zu berichtigen, zu löschen oder zu sperren. Sollten Datenanpassungen durch Updates oder Fehlerbehebung zwingend erforderlich sein, so ist Art und Umfang dem Auftraggeber zuvor schriftlich mitzuteilen.

Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. KONTROLLEN UND SONSTIGE PFLICHTEN DES AUFTRAGNEHMERS

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 DSG NRW folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß § 32 DSG NRW

bzw. §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Die Wahrung des Datengeheimnisses entsprechend § 6 DSG NRW bzw. § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen § 10 DSG NRW bzw. § 9 BDSG und Anlage.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 22 DSG NRW bzw. § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 33, 34 DSG NRW bzw. §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und gegebenenfalls notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

6. UNTERAUFTRAGSVERHÄLTNISSE

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:
- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.
- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

Der Auftragnehmer hat nach Zustimmung des Auftraggebers die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen:
- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 DSG i.V.m. Nr. 6 der Anlage zu § 10 DSG NRW beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
Folgende Firmen sind bei Vertragsabschluss als Unterauftragsnehmer definiert: xyz

7. KONTROLLRECHTE DES AUFTRAGGEBERS

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 10 DSG NRW vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 DSG NRW vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 10 DSG NRW und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

8. MITTEILUNG BEI VERSTÖSSEN DES AUFTRAGNEHMERS

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Einvernehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort, den	Ort, den
AUFTRAGGEBER	AUFTRAGNEHMER

ANLAGE ZUR VEREINBARUNG NACH § 11 DSG NRW: ALLGEMEINE TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN NACH § 10 DSG NRW UND § 9 BDSG – ANLAGE

DER AUFTRAGNEHMER IST VERPFLICHTET, DIE FOLGENDEN TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN ZUR SICHERSTELLUNG DES DATENSCHUTZES ZU ERGREIFEN:

1. Zutrittskontrolle

Die Büroräume des Auftragnehmers, in welchen sich die Systeme befinden, die den Zugriff auf die Komponenten des Auftraggebers ermöglichen, sind gegen den unberechtigten Zugang Dritter in geeigneter Art und Weise zu schützen (Schloss, elektronische Zutrittskontrolle etc.).

2. Zugangskontrolle

Das Eindringen Unbefugter in die EDV-Systeme des Auftraggebers ist zu verhindern.
Hierfür sind folgende technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung festgelegt:

- Die Computersysteme des Auftragnehmers, welche einen Zugriff auf die Rechner und das Netzwerk des Auftraggebers haben, sind mit Passwörtern zu schützen. Die Passwörter haben hierbei eine Mindestlänge von 12 Zeichen zu haben. Weiterhin muss das Passwort mindestens eine Zahl und ein Sonderzeichen beinhalten. Die Passwörter sind regelmäßig zu ändern.
- Die Arbeitsstationen des Auftragnehmers, welche einen Zugriff auf die Systeme des Auftraggebers haben, sind beim Verlassen des Arbeitsplatzes zu sperren (automatisch oder manuell).
- Die Datenverbindung vom Auftragnehmer zum Auftraggeber ist zu verschlüsseln (VPN-Tunnel). Die eingetragenen preshared Keys sind beim Auftragnehmer an sicherem Ort zu verwahren (Tresor).
- Die Zugriffe auf die Domänenstruktur des Auftraggebers dürfen ausschließlich personalisiert erfolgen.
- Sollten Datenträger zwischen Auftragnehmer und Auftraggeber ausgetauscht werden müssen, so sind diese nach dem gängigen Standard zu verschlüsseln.

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in EDV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Es ist eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung zu implementieren. Da alle Zugriffe des Auftragnehmers mit administrativen Rechten erfolgen müssen, sind diese seitens des Auftragnehmers entsprechend zu dokumentieren. Datenveränderungen und Löschungen dürfen nur nach vorheriger Abstimmung mit dem Auftraggeber erfolgen.

4. Weitergabekontrolle

Alle Daten sind auf dem Transportweg, gleich ob dieser leitungs- oder datenträgergebunden ist, nach aktuellen Verfahren zu verschlüsseln. Der Versand von Datenträgern ist zu protokollieren.

5. Eingabekontrolle

Datenveränderungen und Löschungen dürfen nur nach vorheriger Abstimmung mit dem Auftraggeber erfolgen. Weiterhin sind alle Änderungen revisionssicher zu dokumentieren.

6. Auftragskontrolle
Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer: Der Auftragnehmer darf keinerlei Datenänderungen mit personenbezogenem Inhalt ohne Einzelauftrag vollziehen. Eine Auftragserteilung erfolgt grundsätzlich in Schriftform (E-Mail, Fax). Jegliche Änderung ist nach Beauftragung zu dokumentieren.

Weiterhin ist vor dem Beginn der Änderungen eine Datensicherung zu erstellen, welche nach gängigem Standard zu verschlüsseln ist. Der Auftraggeber behält sich vor, die Vorgänge mit einer Vorankündigung von 14 Tagen zu prüfen.

7. Verfügbarkeitskontrolle
Der Auftragnehmer hat Maßnahmen zur Datensicherung (physikalisch/logisch) zu treffen, um die Daten gegen Zerstörung oder Verlust zu schützen. Dies geschieht unter anderem durch:
1. Backup-Verfahren (täglich/wöchentlich)
2. Spiegeln von Festplatten, z.B. RAID-Verfahren
3. Unterbrechungsfreie Stromversorgung (USV)
4. Getrennte Aufbewahrung
5. Virenschutz/Firewall
6. Notfallplan
7. Einsatz von Virenschutzsystemen auf den Clientrechnern und sonstigen relevanten Systemen
8. Einsatz von Firewall-Systemen auf dem Client sowie Server und am Gateway

8. Trennungskontrolle
Der Auftragnehmer hat Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken zu treffen. Dies geschieht unter anderem durch:
1. «Interne Mandantenfähigkeit»/Zweckbindung
2. Funktionstrennung/Produktion/Test
3. Getrennte Speicherung

Die Daten des Auftraggebers dürfen insbesondere nicht mit anderen Informationen vermischt oder genutzt werden.

9. Organisationskontrolle
Der Auftragnehmer muss seine interne Organisation dergestalt führen, dass sie den Anforderungen dieses Vertrages genügt. Dies geschieht unter anderem durch:
1. Interne Datenverarbeitungsrichtlinien und -verfahren, Arbeitsanweisungen, Prozessbeschreibungen und Regelungen für Tests und Freigabe neuer Verfahren, sofern die vom Auftraggeber übermittelten Daten betroffen sind.
2. Nutzung von branchenüblichen Standardsystemen und Programmprüfung sowie geeigneter Individualsoftware.
3. Formulierung eines Notfallplans

10. Weisungskontrolle
Die vom Auftraggeber an den Auftragnehmer übermittelten Daten dürfen ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers verarbeitet werden. Dies geschieht unter anderem durch:
1. Für die Mitarbeiter des Auftragnehmers bindende Richtlinien und Arbeitsanweisungen, die sich aus dem jeweiligen Verfahren ergeben.
2. Auskunftserteilung gegenüber dem Auftraggeber zu speziellen Verfahren oder Daten des Auftraggebers auf Anfrage.