Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 DSGVO

München, 07.05.2020

LITTERA Software & Consulting GmbH
Landshuter Allee 8-10
80637 München
- vertreten durch Herrn Albert Unterkircher als Geschäftsführer -

(nachfolgend „Auftragnehmer“ genannt)

übernimmt gegenüber

Schule: ……...……..
Adresse: ……...……..
PLZ / Ort: ……...……..
- vertreten durch die Schulleitung Herrn/Frau [Vorname, Nachname] -

Kundennummer:……..
(nachfolgend „Auftraggeber“ genannt)

die nachfolgenden datenschutzrechtliche Rechte und Pflichten als Auftragsverarbeiter i.S. von Art. 28 Abs. 3 DS-GVO, wenn und soweit die Hauptleistungen des Auftragnehmers

1. die Wartung und das Hosting der Onlinerecherche „LITTERA web.OPAC“,
2. einen (Fern)wartungszugriff oder
3. eine Bereitstellung von Daten zur Datenkonvertierung oder zur Datenanalyse,

unter der an den Auftraggeber als Kunden vergebenen Kundennummer geschlossene Verträge (insbesondere Softwarelizenzverträge, die die Nutzung von Littera web.OPAC und einen 2nd-Level-Support mitumfassen), auch eine Datenverarbeitung im Auftrag und auf Weisung des Auftraggebers beinhaltet.
Beim Auftragnehmer ist als Datenschutzbeauftragter Herr Albert Unterkircher, Landshuter Allee 8-10, 80637 München, a.unterkircher@littera.eu wirksam bestellt. Bei dem Auftraggeber ist als Datenschutzbeauftragte(r) [Name, dienstliche Kontaktdaten des schulischen Datenschutzbeauftragten] wirksam bestellt.

1. VERTRAGSGEGENSTAND

Der Auftraggeber nutzt für die schulische Lernmittel- und/oder Bibliotheksverwaltung die vom Auftragnehmer an die Erfordernisse der hessischen Schulen angepassten Softwareprogramme „LITTERA Windows für MS-SQL-Server“ (Schulbibliotheksverwaltung) und/oder „LITTERA LM für MS-SQL-Server“ (Lernmittelverwaltung). Für den Auftraggeber besteht in Verbindung mit der Nutzung von „LITTERA Windows für MS-SQL-Server“ die Möglichkeit, auch die Onlinerecherche-Software „LITTERA web.OPAC“, welche vom Auftragnehmer auf einem Webserver betrieben wird und welche für die Nutzer Literaturrecherche und ein Online-Management der ausgeliehenen Bücher bereitstellt, zu nutzen bzw. zur Nutzung anzubieten.

Weiter besteht für den Auftraggeber die Möglichkeit, anlassbezogen – wenn der durch das Land Hessen bereitgestellte 1rst-Level Support durch die EDV-Servicestelle für Schulbibliotheken in Hessen der Hessischen Lehrkräfteakademie nicht ausreicht -einen technischen 2nd-Level-Support in Anspruch zu nehmen, welcher dazu dient, den Ansprüchen an die Funktionsfähigkeit der Softwareprograme, u. a. hinsichtlich der Verfügbarkeit der personenbezogenen Daten Rechnung zu tragen und welcher Fernwartung und ggf. Datenkonvertierungen bzw. Datenanalysen nach den Wünschen des Auftraggebers zwecks Problemlösung umfasst.

Nach den vom Auftraggeber vorgenommenen Nutzungen ist es nicht ausgeschlossen, dass der Auftragnehmer dabei personenbezogene Daten für den Auftraggeber verarbeitet. Dabei verfolgt der Auftragnehmer keine eigenen Zwecke im Umgang mit diesen Daten des Auftraggebers. Vielmehr erfolgt diese Verarbeitung von personenbezogenen Daten des Auftraggebers ausschließlich „im Auftrag und auf Weisung" für die Zwecke des Auftraggebers.

Zu 1.: Der Auftragnehmer bietet standardisierte Produkte des Webhostings für das Softwareprogramm „LITTERA Web.OPAC" für die Onlinerecherche in Schulbibliotheksbeständen an und stellt dem Auftraggeber die technische Umgebung, regelmäßige Aktualisierungen der Recherchesoftware „LITTERA web.OPAC" und die Anbindung an das Internet zur Verfügung.
Zu 2 und 3.: Im Rahmen der Fernwartung oder anlassbezogenen Datenkonvertierung und Datenanalyse erfolgen Zugriffe des Auftragnehmers auf (ggf. personenbezogene) Daten aus Datenbeständen des Auftraggebers zu LITTERA LM und/oder LITTERA Windows ggf. im Rahmen von technischen Hilfestellungen (Supportleistungen), die der Auftraggeber vom Auftragnehmer verlangt. Dies betrifft zum Beispiel die Löschung oder die Sicherung von Daten.

Der Auftraggeber ist als Verarbeiter von personenbezogenen Daten in erster Linie selbst verantwortlich. Für LITTERAwindows und LITTERA LM erfolgen die regelmäßigen Softwareaktualisierungen durch die Auftraggeberin selbst. Ob und wie er dort personenbezogene Daten verarbeitet, liegt in seiner eigenen Verantwortung. Entsprechend muss der Auftraggeber selbst für „seine" Datenverarbeitungsvorgänge technische und organisatorische Maßnahmen ergreifen, um die Schutzziele aus Art. 32 DS-GVO zu erreichen.

Im Zusammenhang mit der Vertragsbeziehung unterrichten sich Auftragnehmer und Auftraggeberin unverzüglich schriftlich oder textlich per E-Mail über datenschutzrelevante Unregelmäßigkeiten, Vorfälle und Verstöße gegen die vertraglichen Regelungen. Die Auftraggeberin behält sich ein Weisungsrecht über die Datenverarbeitung vor.

Datenkategorien im Rahmen des web.OPAC Hosting

Folgende Datenkategorien werden im Rahmen des web.OPAC Hosting verarbeitet:

- Nutzerdaten (Es werden im Rahmen des Hosting des web.OPAC Hessen folgende personenbezogenen Daten der Nutzer verarbeitet: a. Lesernummer, b. Bibliotheksnummer oder Lernmittelverwaltungsnummer, c. nach dem Stand der Technik bcrypt-verschlüsseltes Kennwort),
- Katalog
- Ausleihen (aktuelle)
- Reservierungen (aktuelle)
- Verlängerungen (aktuelle)
- Merklisten (aktuelle)
- historische Verleihdaten (die letzten drei Ausleihen, inklusive der aktuellen)
- IP-Adresse (des aufrufenden Rechners)

Die mit den Webhosting-Dienstleistungen verbundenen Verarbeitungsarten umfassen eine regelmäßige Speicherung und Löschung von Daten sowie die Anbindung der Daten an das Internet.

(1) Datenkategorien im Rahmen der anlassbezogenen Fernwartung bzw. Datenanalysen und Datenkonvertierungen

- Es werden im Rahmen der anlassbezogenen (Fern)-wartung ggf. – wenn unbedingt erforderlich – neben Lesernummer, Bibliotheks- oder Lernmittelverwaltungsnummer und verschlüsseltem Kennwort

- A. von den Schülerinnen und Schülern sowie ausleihenden Lehrkräften folgende personenbezogene Daten (LITTERA Windows) verarbeitet:
- Vorname, Name, Geburtsdatum, Klasse, ID, ggf. E-Mail-Adresse und Foto (soweit erhoben),
-
- B. von den Schülerinnen und Schülern und Eltern folgende personenbezogene Daten (LITTERA LM) verarbeitet:
    a. SchuelerId
    b. Nachname
    c. Geschlecht
    d. Vorname
    e. Telefon1
    f. Geburtsdatum
    g. Klassenname
    h. StrasseHausnummer
    i. PLZ
    j. Ort
    k. Anrede
    l. Vorname2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    m. Nachname2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    n. StrasseHausnummer2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    o. PLZ2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    p. Ort2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    q. Anrede2 (Erziehungsberechtigter für Beschädigungen/Verluste)
    r. Kurse

- von den Bibliothekskräften folgende personenbezogene Daten (LITTERA Windows) verarbeitet:

    a. Benutzername
    b. Kennwort
    c. Kürzel
    d. Vorname
    e. Nachname

(2) Ausgestaltung der Fernwartung und Datenkonvertierungen und Datenanalysen

(1) Bei jeder Fernwartung ist der Zugriff auf personenbezogene oder sonst vertrauliche Daten bzw. deren Übermittlung auf das absolut erforderliche Minimum zu beschränken. Eine Fernwartung, die die Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener oder sonst vertraulicher Daten gefährden könnte, darf nicht erfolgen, selbst wenn die sonstigen Anforderungen dieses Vertrages erfüllt sind. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen als die vertraglich vereinbarten Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(2) Die Fernwartung erfolgt anlassbezogen im Auftrag des Auftraggebers. Da aus SQL-Server-Datenbanken aus technischen Gründen keine Daten aus der Anwendung heraus verschickt werden können, muss der/die schulische Bibliotheksleiter/in eine externe Datensicherung erstellen und über einen verschlüsselten (mindestens TLS 1.2) Upload an den Auftragnehmer schicken. Der Auftragnehmer stellt hierfür einen entsprechenden Link zur Verfügung, der einen verschlüsselten Upload nach dem Stand der Technik erlaubt.

- Für die Fernwartung dürfen nur betriebliche/dienstliche Rechner genutzt werden.
- Die Fernwartungsmaßnahme ist sowohl von dem Auftraggeber als auch vom Auftragnehmer vorab zu dokumentieren (mit persönlichem Zugangsaccount der ausführenden Person, Datum, Uhrzeit, Herkunft und Art der betroffenen Daten und nachträglich auch der ausgeführten Tätigkeiten) und –nach vorheriger Information der ausführenden Mitarbeiterinnen und Mitarbeiter – im System zu protokollieren. Die Protokollierung durch den Auftragnehmer erfolgt im internen Kundenverwaltungssystem.
- Die Datenübertragung darf nur erfolgen, wenn die Daten beim Auftragnehmer auf dem Fernwartungsrechner - getrennt von anderen Datenbeständen - gespeichert und unverzüglich gelöscht werden, sobald sie nicht mehr erforderlich sind. Ausdrucke sind unverzüglich im Aktenvernichter zu zerstören.

2. DAUER DER VEREINBARUNG UND AUßERORDENTLICHES KÜNDIGUNGSRECHT

Die Vereinbarung ist auf unbestimmte Zeit geschlossen, richtet sich im Übrigen nach der Dauer des Softwarelizenzvertrages und kann von beiden Parteien mit der für den Softwarelizenzvertrag vereinbarten Frist https://www.littera.eu/agb/ gekündigt werden. Beide Parteien können den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn die jeweils andere Partei ihren Pflichten aus diesem Vertrag nicht nachkommt oder Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

3. VERGÜTUNG FÜR DIE LEISTUNGEN DER AUFTRAGSVERARBEITUNG

(1) Der Abschluss des Auftragsverarbeitungsvertrags ist kostenfrei, sofern das bereitgestellte Vertragsmuster des Auftragnehmers verwendet wird.

(2) Tätigkeiten nach spezieller Weisung des Auftraggebers
Erfolgen Tätigkeiten der Verarbeitung des Auftragnehmers im Datenbestand des Auftraggebers aufgrund einer entsprechenden Weisung, so weist der Auftragnehmer den Auftraggeber schriftlich auf eine eventuelle Kostenpflicht vor der Durchführung des Auftrags hin und vereinbart die entsprechende Vergütung.

4. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer bestehen

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage 1 zu entnehmen). Die technischen und organisatorischen Maßnahmen sind im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung anzupassen.

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung, Einschränkung der Verarbeitung und Löschung, Datenübertragbarkeit, Widerspruch und Widerruf) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die/den Verantwortliche/n des Auftraggebers (Schulleitung) bestätigt oder geändert wird.

(10) Sollten Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen (etwa durch Pfändung und Beschlagnahme), durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(11) Ein Zurückbehaltungsrecht des Auftragnehmers besteht hinsichtlich der verarbeiteten Daten nicht.

5. PFLICHTEN DES AUFTRAGGEBERS

(1) Der Auftraggeber ist für eine Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten durch ihn auf den IT-Systemen des Auftragnehmers sowie der Wahrung von Rechten der Betroffenen verantwortlich. Der Auftraggeber hat dafür Sorge zu tragen, dass die gesetzlich oder behördlich vorgeschriebenen Voraussetzungen für „seine" Datenverarbeitungen geschaffen werden bzw. Anforderungen erfüllt werden, wie bspw.:
   a. die Einhaltung von Löschfristen
   b. die zulässige Speicherdauer
   c. das Einholen von Einwilligungserklärungen

(2) Die Parteien stellen sich gegenseitig von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. (Art. 82 DS-GVO bleibt unberührt).

6. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Sämtliche Auftragsverarbeitungsleistungen des Auftragnehmers werden ausschließlich in Deutschland oder Österreich erbracht, nach vorheriger Zustimmung des Auftraggebers kommt auch die Erbringung in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum in Betracht. Jede Verlagerung dieser Dienstleistungen oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und setzt das Vorliegen eines angemessenen Datenschutzniveaus voraus.

7. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

1. LITTERA Software & Consulting GmbH
   Haller Au 19a
   6060 Hall in Tirol

   Art der Tätigkeiten: Dienstleistung in Datenverarbeitung und Informationstechnik; Unternehmensberatung.

   Orte der Leistungserbringung: Die Leistungen werden ausschließlich in Österreich und/oder in Deutschland erbracht.

2. ALL-INKL.COM
   Neue Medien Münnich Inhaber: René Münnich
   Hauptstraße 68
   02742 Friedersdorf, Deutschland

   Art der Tätigkeiten: Webhosting und Domainverwaltung
   Orte der Leistungserbringung: Die Leistungen werden ausschließlich in Österreich und/oder in Deutschland erbracht.

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

8. HAFTUNGSAUSSCHLUSS

Dieses Dokument wurde nach bestem Wissen erstellt. Der Auftragnehmer übernimmt keine Haftung für die Vollständigkeit und Richtigkeit der Ausführungen. Eine rechtskonforme Umsetzung der DSGVO erfordert die Umsetzung der Richtlinie in allen betroffenen Bereichen des Auftraggebers, wie internes Netzwerk, Zugriffs- und Zutrittsberechtigungen, Mitarbeiterschulungen und -vereinbarungen, etc.

9. GELTENDES RECHT

Diese Vereinbarung unterliegt ausschließlich dem Recht der Bundesrepublik Deutschland. Sollte eine der Bestimmungen nichtig sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt.

Wir bitten um die Bereitstellung von zwei unterzeichneten Ausführungen – Sie erhalten ein unterzeichnetes Dokument retour.

Auftraggeber:	Auftragnehmer:
Datum:	Datum:
Unterschrift:	Unterschrift:

ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOMS)

VERTRAULICHKEIT

- **Zutrittskontrolle**

Elektronische Zutrittskontrollsysteme überwachen und gewährleisten den autorisierten Zutritt, in denen die IT-Systeme für den Kunden betrieben bzw. administriert werden.

Zutritte von Besucherinnen und Besuchern werden stets durch Beschäftigte des Auftragsverarbeiters begleitet.

Der Eingangsbereich, in dem die Administration erfolgt, ist mit Videokameras ausgestattet.

Die Zutrittsberechtigung ist für die Beschäftigten organisatorisch festgelegt, Magnetkarten bzw. Schlüssel werden nur entsprechend einer Organisationsanweisung vergeben.

Regelungen für Fremdpersonal und zur Begleitung von Gästen sind vorhanden.

Sonstige Maßnahmen: Zutrittsberechtigungsmanagement; Abschließbare Möbel; Clear Desk; Alarmierungssysteme; Regelungen für Besucherinnen und Besucher; Sonstige Maßnahmen wie Audit etc.

- **Zugangskontrolle**:

Durch die Verwehrung des Zugangs zu Datenverarbeitungssystemen, mit denen die (Auftrags-) Verarbeitung durchgeführt wird, für Unbefugte wird die Zugangskontrolle gesichert.

Maßnahmen:
Der Zugang zu Datenverarbeitungssystemen ist nur durch Authentifizierung möglich (mindestens durch Benutzername und Passwort).
Zugänge durch ein Berechtigungskonzept (abgestufte Zugriffsberechtigungen) sind autorisierten Beschäftigten vorbehalten.

Sonstige Maßnahmen: Bildschirm- und Gerätesperren; Schadsoftware-Scanner; Absicherung von Fernzugriffen; Firewalls; Netzwerksegmentierung; Verschlüsselung von Daten während der Übertragung; Zugangsprotokollierung; Sonstige Maßnahmen wie Audit etc.

- **Datenträgerkontrolle:**

Räume zur Lagerung und Archivierung von Datenträgern; Verwaltung von Kopien; Sichere Löschung von Daten und Datenträgern; Sichere Vernichtung von Datenträgern; Sonstige Maßnahmen wie Audit etc.

- **Speicherkontrolle:**

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.
Trennung von Produktivdaten und Testdaten; Trennung von Benutzerdaten; Mandantenfähigkeit von Speichersystemen; Sonstige Maßnahmen wie Audit etc.

- **Zugriffskontrolle**:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten.
Die Beschäftigten des Auftragsnehmers sind zum Schutz personenbezogener Daten geschult und entsprechend zur Vertraulichkeit verpflichtet.

Sonstige Maßnahmen: Zugriffsberechtigungsmanagement; Umgang mit privilegierten Rechten

- **Übertragungskontrolle:**

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können:
Regelungen für zulässige und unzulässige Übermittlungen; Regelungen für Übermittlungswege und Empfänger; Dokumentation der eingesetzten Übermittlungsprogramme; Sonstige Maßnahmen wie Audit etc.

- **Pseudonymisierung**:

Es ist Sache des Auftraggebers personenbezogene Daten selbst zu pseudonymisieren, soweit dies gesetzlich erforderlich ist.

- **Klassifikationsschema für Daten:**

Aufgrund der Selbsteinschätzung werden die Daten als vertraulich eingestuft.

INTEGRITÄT

- **Weitergabekontrolle**:

Es erfolgt eine verschlüsselte Verschlüsselung der Datenübertragung nach aktuellem Stand, mindestens nach Standard SSL/TLS 1.2 (https).

- **Eingabekontrolle**:

Eine Eingabekontrolle ist vom Auftraggeber organisatorisch sicherzustellen.

- **Verfügbarkeit**

Es erfolgt die Anfertigung von Sicherheitskopien von Daten (mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum)

Einsatz einer unterbrechungsfreien Stromversorgung
Standardprozesse bei Wechsel/Ausscheiden von Mitarbeiterinnen und Mitarbeitern

Der Datenbestand ist durch geeignete Sicherungsmaßnahmen der Quelldatenbank in LITTERA Windows / LITTERA LM seitens des Auftraggebers, also durch den schulischen Bibliotheksleiter, sicherzustellen.

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Eine ausführlichere Auflistung der beim Auftragsverarbeiter getroffenen Technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung ist in der

1. bei der EDV-Servicestelle für Schulbibliotheken in Hessen bei der Lehrkräfteakademie,
2. bei der Datenschutzbeauftragten des Hessischen Kultusministeriums und
3. beim Datenschutzbeauftragten des Auftragsverarbeiters
vorgehaltenen Anlage – Technische und organisatorische Maßnahmen beim Auftragnehmer enthalten. Diese Anlage wurde ebenfalls dem HBDI zur Prüfung vorgelegt.

Getroffene Maßnahmen:

Datenschutz-Management
Regelmäßige Schulung der Beschäftigten

Der Auftragsverarbeiter setzt einen Kernbestand an dauerhaft beschäftigtem Personal mit DV-technischer Erfahrung und entsprechendem Expertenwissen ein.