

Lizenz- und Dienstleistungsvertrag SchoolUpdate

abgeschlossen zwischen

<p>bit media education solutions GmbH Kärntner Straße 337 A-8054 Graz, Austria (nachfolgend „Lizenzgeber“ bzw. „Auftragsverarbeiter“ genannt)</p>
--

und

Schule:	
Schulkennzahl:	
Adresse:	
PLZ Ort:	
Ansprechperson:	
Telefon:	
E-Mail:	
(nachfolgend „Lizenznehmer“ bzw. „Kunde“ genannt)	

(gemeinsam „Vertragspartner“ genannt)

Anlage:

Anhang A: Auftragsvereinbarung gem. Art. 28 EU-DSGVO

1 Präambel

SchoolUpdate (nachfolgend „Lizenzprodukt“ genannt) ist gleichzeitig Mobile App und Web-Anwendung, speziell entwickelt für die Verbesserung der Kommunikation zwischen Schule, Lehrern und Eltern.

Das System wird vom Lizenzgeber als webbasierte Lösung sowie als Mobile App zur Nutzung durch Schulen, Lehrpersonen, Eltern und Erziehungsberechtigte angeboten und betrieben. Voraussetzung für die Nutzung des Lizenzprodukts ist ein aufrechter Lizenz- und Dienstleistungsvertrag.

Der Zugang zum Softwareprodukt erfolgt entweder online unter Verwendung eines Standard-Webrowsers auf Desktop-PC sowie auf Smartphones als Mobile App für IOS und Android.

2 Lizenzvereinbarung

bit media räumt dem Kunden im Rahmen dieser Lizenz- und Dienstleistungsvereinbarung das zeitlich auf die Dauer dieser Vereinbarung begrenzte, nicht ausschließliche und nicht übertragbare Recht ein, das Softwareprodukt gemäß den nachfolgenden Bestimmungen zu nutzen. Details zum Entgelt befinden sich in Pkt. 5 dieser Vereinbarung.

Das Produkt SchoolUpdate ist urheberrechtlich geschützt. Das Lizenzprodukt kann auf beliebigen PC-Arbeitsplätzen und für die Nutzung geeigneten mobilen Endgeräten durch eine beliebige Anzahl an Personen der eigenen Schule sowie durch Eltern und Erziehungsberechtigte der Schüler:innen genutzt werden.

Der Zugang zum Lizenzprodukt darf ausschließlich über einen personalisierten Zugang (persönlicher Username und Passwort) erfolgen. Öffentliche oder anonymisierte Zugänge zum Lizenzprodukt sind untersagt.

SchoolUpdate Premium - Funktionsliste:

- Nachrichtenversand (inkl. Übersetzung)
- Abwesenheiten melden
- Kalender
- Empfehlungen
- Hausaufgaben
- Listen & Umfragen
- Elternsprechtage planen
- Versenden von Notfallnachrichten

3 Leistungen des Lizenzgebers

3.1 Einrichtung & Freischaltung

Der Lizenzgeber wird nach Bestellung durch den Kunden eine schulspezifische Instanz des Lizenzprodukts einrichten und zur Nutzung über Internet freischalten. Nach erfolgter Freischaltung werden die Zugangsdaten an den Lizenznehmer übermittelt.

3.2 Betrieb & Wartung

Der Lizenzgeber verpflichtet sich, das Lizenzprodukt im Rahmen dieser Vereinbarung durchgehend zu betreiben, technisch zu warten, bekannte Fehler zu beheben und insbesondere auf neu herauskommende Betriebssysteme und Browserversionen anzupassen.

Darüber hinaus wird der Lizenzgeber das Lizenzprodukt softwaretechnisch warten und weiterentwickeln, um den Einsatz der Software auch bei technologischen Änderungen zu gewährleisten.

Die Umsetzung der Wartungsleistungen erfolgt durch eine zeitgerechte Bereitstellung von

Programmupdates auf dem Server des Lizenzgebers bzw. in den jeweiligen App-Stores. Zeitpunkt der Einführung und Umfang der Verbesserung liegen im Ermessen des Lizenzgebers.

3.3 Hotline & Support

Mit unserer Hotline bieten wir allen Lizenznehmern eine Unterstützung beim Einsatz des Lizenzprodukts. Die Hotline ist telefonisch unter der Tel-Nr. 0316 / 286 186 zu den auf der Website angeführten Zeiten sowie per Mail unter support@schoolupdate.com. Anfragen werden entweder telefonisch oder per E-Mail beantwortet. Die Hotline steht nicht an gesetzlichen Feiertagen, an schulfreien Tagen, eingeschränkt an Fenstertagen, im Zeitraum zwischen 24.12. und 6.1. des Folgejahres sowie für einen Zeitraum von fünf Wochen während der Sommerferien zur Verfügung.

4 Nicht enthaltene Leistungen

Nicht im Leistungsumfang enthalten sind Maßnahmen zur Pflege des Datenbestandes, z.B. Datenimporte aus anderen Softwareprodukten (ausgenommen SOKRATES) oder sonstigen externen Datenquellen, Bereinigung von Eingabefehlern etc.) sowie Leistungen für die Umsetzung schulspezifischer Anforderungen und Schulungen. Derartige Leistungen können vom Kunden bei bit media gesondert zu den jeweils gültigen Preisen beauftragt werden.

5 Entgelt

Das Entgelt für die Nutzung des Lizenzprodukts besteht aus einer jährlichen Nutzungsgebühr in Abhängigkeit der Schulgröße.

Jährliche Gebühren:

Beschreibung	Schulkennzahl	Preis *)
SchoolUpdate - Premium Lizenz, Betrieb, Wartung & Support (bis 30 Schüler:innen)		60,00
SchoolUpdate - Premium Lizenz, Betrieb, Wartung & Support (bis 100 Schüler:innen)		160,00
SchoolUpdate - Premium Lizenz, Betrieb, Wartung & Support (über 100 Schüler:innen)		220,00
Summe jährliche Gebühren		0,00

Alle Preise in EUR exkl. 20% MwSt.

*) Es wird Wertbeständigkeit des Entgelts vereinbart. bit media ist berechtigt, das Entgelt jährlich gem. Verbraucherpreisindex der Statistik Austria (VPI 2020) zu erhöhen, mindestens jedoch um 1,5% p.a.

6 Zahlungsmodalitäten

Die jährliche Nutzungsgebühr wird bei Vertragserrichtung bzw. in den Folgejahren zu Beginn des Vertragsjahres in Rechnung gestellt. Die Bezahlung von Rechnungen erfolgt binnen 14 Tagen ohne Abzug.

7 Änderungen

Änderungen und Abweichungen hinsichtlich der Anzahl von bis zu 10 SchülerInnen bleiben unberücksichtigt. Darüber hinaus gehende Änderungen bedürfen einer Änderungsvereinbarung.

8 Laufzeit

Diese vorliegende Vereinbarung tritt mit dem Datum der Unterzeichnung durch den Kunden in Kraft und ist auf unbestimmte Zeit abgeschlossen. Die Vereinbarung kann von Kunden sowie vom Lizenzgeber unter Einhaltung einer Kündigungsfrist von drei Monaten auf das Ende eines Kalenderjahres schriftlich widerrufen oder gekündigt werden. Mit der Kündigung erlischt das Recht an der Nutzung des Lizenzprodukts. Die bei Inkrafttreten der Kündigung im System vorhandenen Daten können dem Kunden in maschinenlesbarer Form auf einem Datenträger zur Verfügung gestellt werden.

9 Haftung

Wenngleich die vertragsgegenständliche Software sorgfältigen Qualitätssicherungsmaßnahmen unterliegt, können Mängel und Fehler nicht ausgeschlossen werden. Für die Fehler- und Mängelbehebung gelten die Bestimmungen dieses Vertrags sowie die allgemeinen gesetzlichen Gewährleistungsbestimmungen.

Der Lizenzgeber haftet jedoch nicht für Schäden oder Folgeschäden, die auf Grund der Benutzung des Lizenzprodukts entstehen. Insbesondere nicht für Personen-, Sach- oder Vermögensschäden, die als Folgeschäden unmittelbar und/oder mittelbar im Zusammenhang mit der Nutzung des Lizenzprodukts in Verbindung stehen. Dies gilt nicht bei Vorsatz oder grober Fahrlässigkeit.

10 Geltendes Recht

Diese Vereinbarung unterliegt österreichischem Recht. Gerichtsstand ist das sachlich zuständige Gericht in Graz.

Auftragsbestätigung

Bitte per Mail zurücksenden an denise.ragger@bitmedia.at.

.....
Ort, Datum

.....
Unterschrift/Stempel

- Rechnung an Kundenadresse (gem. Seite 1):
- Rechnung an alternative Adresse:

.....

.....

.....

Anhang A – Vereinbarung zur Auftragsverarbeitung gemäß Art. 28

DSGVO

1 Präambel

Hinsichtlich der Bestimmungen der Lizenz- und Dienstleitungsvereinbarung ist der Lizenzgeber „Auftragsverarbeiter“ und der Kunde „Verantwortlicher“ im Sinne der DSGVO. Betreffend der Leistungserbringung gelten die folgenden Bestimmungen zur Auftragsverarbeitung.

2 Auftragsverarbeitung

Die Auftragsverarbeitung durch den Auftragsverarbeiter beinhaltet folgende Leistungen:

- Zurverfügungstellung des Lizenzprodukts im Rechenzentrum des Auftragsverarbeiters, sowie als Mobile App, basierend auf den Bestimmungen des Lizenz- und Dienstleistungsvertrags.
- Betrieb, Wartung und Support im Rahmen der Nutzung des Lizenzprodukts basierend auf den Bestimmungen dieses Lizenz- und Dienstleistungsvertrages und dieses Anhangs.

2.1 Art und Zweck der Verarbeitung von Daten

Verantwortlicher

Die Datenverarbeitung durch den Verantwortlichen dient der digitalen Kommunikation der Schule bzw. Lehrpersonen mit Eltern und Erziehungsberechtigten. Bestandteil der Kommunikation sind Textmitteilungen mit oder ohne Anhang, Abwesenheitsmeldungen, Termine sowie Informationen zu sonstigen Anlässen und Ereignissen im Schulalltag.

Für den Betrieb dieses Service sind Schülerdaten (Vorname, Nachname, Geschlecht, Geburtsdatum, Klassenzugehörigkeit) sowie Daten von Lehrpersonen und Eltern/Erziehungsberechtigten (Username, Passwort, ggf. Telefon und E-Mail) erforderlich.

Rechtsgrundlage für die Verarbeitung der Daten von Schülern sowie Eltern und Erziehungsberechtigten sind die schulrechtlichen Bestimmungen sowie Einwilligungen der Betroffenen. Rechtsgrundlage für die Verarbeitung von Personendaten von Lehrpersonen sind die schulrechtlichen Bestimmungen sowie das berechtigte Interesse des Verantwortlichen.

Auftragsverarbeiter

Der Zweck der Datenverarbeitung beim Auftragsverarbeiter beschränkt sich auf den Serverbetrieb und die Wartung der Anwendung sowie auf die Anwendungsunterstützung (Hotline, Support) und ggf. erforderliche Tätigkeiten zur Fehleranalyse.

Die Daten werden vom Auftragsverarbeiter ausschließlich im Sinne der vertraglichen Vereinbarung verarbeitet und auf Weisung des Auftraggebers bearbeitet. Eine Weitergabe oder Zweckentfremdung der Daten durch den Auftragsverarbeiter ist ausgeschlossen.

2.2 Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Schüler
- Lehrpersonen
- Eltern/Erziehungsberechtigte

Folgende Datenkategorien werden verarbeitet:

Schülerdaten:

- Vorname
- Nachname
- Geburtsdatum
- Geschlecht

Lehrerdaten:

- Titel (optional)
- Vorname(n)
- Zuname
- Geschlecht
- Username
- Passwort
- Adresse (optional)
- E-Mail (optional)
- Telefon (optional)

Eltern/Erziehungsberechtigte:

- Titel (optional)
- Vorname
- Nachname
- Verwandtschaftsbez. zum Kind
- Geschlecht
- Username
- Passwort
- Adresse (optional)
- E-Mail (optional)
- Telefon (optional)

3 Dauer der Verarbeitung

Die Verarbeitung erfolgt auf unbestimmte Zeit bzw. steht in Abhängigkeit zu den abgeschlossenen Lizenz-, Wartungs- und Dienstleistungsvereinbarungen. Sie endet nach Kündigung des Vertragsverhältnisses durch den Kunden.

4 Pflichten des Auftragsverarbeiters

4.1 Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Kopien oder Duplikate der Daten 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.

4.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Verwaltungs- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt. Erhält der Auftragsverarbeiter 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 Auftragsverarbeiters eines schriftlichen Auftrages des Auftraggebers.

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. B, 29, 32 Abs. 4 DSGVO.

4.3 Der Auftragsverarbeiter 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 und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

4.4 Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO zu erfüllen. Auf der Webseite des Auftragsverarbeiters „www.bitmedia.at“ sind die Kontaktinformationen des Datenschutzbeauftragten ersichtlich.

4.5 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach den Art 32ff DSGVO insbesondere iVm Art 5 Abs. 1 und Abs. 2 DSGVO ergriffen hat und deren Einhaltung regelmäßig kontrolliert und dokumentiert. Es handelt sich hierbei um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme (Einzelheiten siehe Anlage).

4.6 Mitwirkungspflicht bei Betroffenenrechten: Sofern der Auftraggeber nicht über die technische Möglichkeit verfügt, die Betroffenenrechte nach Kapitel III der DSGVO (insbesondere Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) wahrzunehmen, so unterstützt der Auftragsverarbeiter den Auftraggeber mit notwendigen Informationen, sodass dieser den gesetzlichen Pflichten nachkommen kann.

4.7 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.8 Der Auftragsverarbeiter verpflichtet sich den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten zu unterstützen. Dazu gehören insbesondere:

- a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- e) die Unterstützung des Auftraggebers im Rahmen einer Konsultation mit der Aufsichtsbehörde;

4.9 Auftraggeber und Auftragsverarbeiter haben für die vorliegende Auftragsverarbeitung jeweils ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu führen.

4.10 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 Auftragsverarbeiter verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

4.11 Der Auftragsverarbeiter stellt insbesondere sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch: die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit.

4.12 Der Auftragsverarbeiter ist spätestens nach Beendigung dieser Vereinbarung verpflichtet, sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber zu übergeben und/ oder in dessen Auftrag datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Wenn der Auftragsverarbeiter 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.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

4.13 Der Auftragsverarbeiter hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

5 Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen zum Schutz und zur Sicherheit der Daten unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird.

Die technischen und organisatorischen Maßnahmen liegen als Anhang A bei.

Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

6 Ort der Verarbeitung

Alle Datenverarbeitungstätigkeiten für personenbezogene Daten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt. Dies gilt auch für die Leistungen des Sub-Auftragsverarbeiters gemäß Pkt. 7.

Datenverarbeitungen von nicht-personenbezogenen Daten unterliegen nicht der DSGVO (z.B. Sprachübersetzungen von Inhalten), und können ggf. auch außerhalb der EU bzw. des EWR durchgeführt werden.

7 Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung einer Dienstleistung hinzuziehen:

Infrastrukturprovider: A1 Telekom Austria AG, Marburger Kai 43 – 45, 8010 Graz

Die erforderlichen Vereinbarungen zwischen dem Auftragsverarbeiter und dem Sub-Auftragsverarbeiter gemäß des Art. 28 Abs. 4 DSGVO sind erfüllt.

Jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung durch andere Sub-Auftragsverarbeiter bedarf der vorherigen schriftlichen Genehmigung durch den Auftraggeber.

Es ist sichergestellt, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

8 Technisch-organisatorische Maßnahmen (TOMs)

8.1 Vertraulichkeit

- Zutrittskontrolle (wird über Sub-Auftragsverarbeiter abgedeckt): Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- Zugangskontrolle: Schutz vor unbefugter Systembenutzung: Kennwörter (Richtlinien: keine Mehrfachverwendung, individuelle Richtlinien, Sperre bei mehrfacher Falscheingabe)
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Unterschiedliche Systemrollen einstellbar, spezielle Systemadministrationszugriffe gesondert möglich. Serverzugriff nur eingeschränkt auf Mitarbeiter der Abteilung ICT
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden: Mandantenfähigkeit im System, getrennte Datenbanken bei Premium Systemen.
- Klassifikationsschema für Daten: Intern

8.2 Integrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Verschlüsselung beim Aufruf des Systems (HTTPS), keine weitere Datenübertragung vorgesehen.
- Eingabekontrolle: Systemlogbuch für die Protokollierung von Änderungen im System sowie automatische Systemprozesse

8.3 Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Tägliche Datensicherung (30 Tage rückwirkend) in anderem, Brandabschnitt, Ausfallssicherheit USV, Rasche Wiederherstellbarkeit;
- Lösungsfristen: Datenlöschung nach Vertragsende.

8.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Hosting & Betrieb der Softwarelösung: Überprüfung der Prozesse und Maßnahmen im Rahmen des jährlichen ISO 9001 Qualitätsaudits (QM). Wiederkehrende (jährliche) Risikoanalysen der Serversysteme inkl. Dokumentation. Forderung der ISO 27001 Zertifizierung des Sub-Auftragsverarbeiters.
- Entwicklung und Wartung der Softwarelösung: Durchführung von Sicherheitsüberprüfungen bei jedem Major Release der Software (Version X.1.1), Überprüfung der Einhaltung von Datenschutzrichtlinien bei jedem Minor Release (Version 1.X.1). Definierte Security Richtlinien bei Software-Entwicklung und Kontrolle der Einhaltung durch Code Review Prozess sowie interne und externe ISO 9001 Audits (QM).