**Rahmenvertrag für die Bearbeitung und Nutzung**

**von besonders schützenwerten Personendaten**

zwischen dem **Kanton Thurgau**

vertreten durch

das Amt für Informatik

Im Roos 6

8570 Weinfelden

**als Leistungsbezügerin** (=Bestellerin)

und xxx xxx

Strasse / Nummer

PLZ Ort

**als Leistungserbringerin** (=Lieferantin)

betreffend Verarbeitung von Schülerdaten und Nutzung der

Datenschnittstelle SVS Schulverwaltung (EdIS)

des Amts für Volksschule Thurgau

Inhaltsverzeichnis

[1 Allgemeine Vertragsbestimmungen 3](#_Toc60815672)

[1.1 Vertragszweck, Vertragsgegenstand 3](#_Toc60815673)

[1.2 Vertragsbestandteile und Rangfolge 3](#_Toc60815674)

[1.3 Gegenseitige Information 3](#_Toc60815675)

[1.4 Verantwortlichkeiten Leistungsbezüger 3](#_Toc60815676)

[1.5 Finanzielle Konditionen 4](#_Toc60815677)

[1.6 Haftung 4](#_Toc60815678)

[2 Datenschutz 4](#_Toc60815679)

[2.1 Gesetzlicher Vertragsvorbehalt 4](#_Toc60815680)

[2.2 Datenherr 4](#_Toc60815681)

[2.3 Zweck 5](#_Toc60815682)

[2.4 Datenzugriff durch ausländisches Recht 5](#_Toc60815683)

[2.5 Informationsgesuche 5](#_Toc60815684)

[2.6 Geheimhaltung 5](#_Toc60815685)

[2.7 Kontrollrecht 6](#_Toc60815686)

[2.8 Private Ansprüche 6](#_Toc60815687)

[2.9 Abgrenzung der Datenbearbeitung 6](#_Toc60815688)

[2.10 Unterauftragsverhältnisse 6](#_Toc60815689)

[2.11 Entwicklung und Wartung von Systemen 6](#_Toc60815690)

[2.12 Transparenz über Massnahmen 6](#_Toc60815691)

[2.13 Sanktionen 7](#_Toc60815692)

[2.14 Datenvernichtung 7](#_Toc60815693)

[2.15 Datenportabilität 7](#_Toc60815694)

[3 Sicherheit 7](#_Toc60815695)

[3.1 ISO 27001 7](#_Toc60815696)

[3.2 Anforderungskatalog C5 7](#_Toc60815697)

[3.3 Sicherheitsaktualisierung 8](#_Toc60815698)

[3.4 Datenschutzaktualisierung 8](#_Toc60815699)

[3.5 Vorabkontrolle 8](#_Toc60815700)

[3.6 Vorfall 8](#_Toc60815701)

[3.7 Subunternehmen 8](#_Toc60815702)

[3.8 Datenflussdokumentation 8](#_Toc60815703)

[3.9 Schutzmassnahmen 8](#_Toc60815704)

[3.10 Best Practice 8](#_Toc60815705)

[3.11 Schwachstellenmanagement 8](#_Toc60815706)

[3.12 Logdateien 9](#_Toc60815707)

[3.13 Malwareschutz 9](#_Toc60815708)

[3.14 Zuordnung 9](#_Toc60815709)

[3.15 Private Schlüssel 9](#_Toc60815710)

[3.16 Datentransfer 9](#_Toc60815711)

[3.17 Zugriffsbeschränkung 9](#_Toc60815712)

[3.18 Datenaustausch 9](#_Toc60815713)

[3.19 Identity und Access Management 9](#_Toc60815714)

[3.20 Zwei-Faktor-Authentisierung 9](#_Toc60815715)

[3.21 Zertifikate 10](#_Toc60815716)

[3.22 Firewall 10](#_Toc60815717)

[3.23 Benutzerüberwachung 10](#_Toc60815718)

[3.24 Zeitsynchronisation 10](#_Toc60815719)

[3.25 Kommunikation 10](#_Toc60815720)

[3.26 Sicherheitstests 10](#_Toc60815721)

[3.27 Physische Sicherheit 10](#_Toc60815722)

[3.28 Betriebskontinuität 10](#_Toc60815723)

[4 Schlussbestimmungen 11](#_Toc60815724)

[4.1 Vertragsdauer und Kündigung 11](#_Toc60815725)

[4.2 Salvatorische Klausel 11](#_Toc60815726)

[4.3 Anwendbares Recht und Gerichtsstand 11](#_Toc60815727)

# Allgemeine Vertragsbestimmungen

## Vertragszweck, Vertragsgegenstand

Der vorliegende Rahmenvertrag für die Bearbeitung und Nutzung von besonders schützenwerten Personendaten, nachstehend mit Rahmenvertrag bezeichnet, enthält die generellen Regelungen der Vertragsparteien bezüglich der vom Leistungserbringer zu erbringenden Informatikdienstleistungen.

Diese umfassen die Datenschutz- und Informationssicherheitsbestimmungen für die vom Amt für Volkschule zur Verfügung gestellten Daten und die Verwendung der Datenschnittstelle zwischen der Anwendung SVS Schulverwaltung und der Anwendung des Leistungserbringers.

Die zur Verfügung gestellten Daten dienen der ausschliesslichen Nutzung durch die vom Leistungserbinger betriebene Schulanwendung und der entsprechend vertraglich gebundenen Schulen.

Die Bereitstellung der automatisierten Schnittstelle des Leistungserbingers und des Leistungsbezügers und die Nutzung dieser für den Datentransfer ist integraler Bestandteil dieser Vereinbarung. Sie basiert auf Microsoft BizTalk und wir vom Leistungsbezüger zur Verfügung gestellt.

Die einwandfreie Konnektivität der Anwendung des Leistungserbringers wird vorausgesetzt.

## Vertragsbestandteile und Rangfolge

Bestandteile der vertraglichen Vereinbarungen zwischen den Parteien sind folgende Dokumente:

* Der vorliegende Rahmenvertrag
* Die AGB für IKT-Leistungen der Schweizerischen Informatikkonferenz Ausgabe Januar 2020

Im Falle von Widersprüchen zwischen Vertragsbestandteilen gehen spezielle Regelungen allgemeinen Regelungen vor. Bei gleicher Rangfolge gehen zeitlich jüngere Vereinbarungen zeitlich älteren Vereinbarungen vor.

## Gegenseitige Information

Die Vertragsparteien geben sich gegenseitig Name und Funktion ihrer für die Zusammenarbeit verantwortlichen Mitarbeiterinnen und Mitarbeiter bekannt und bezeichnen ihre Kontaktstellen.

Die Vertragsparteien informieren sich regelmässig gegenseitig über Umstände und Ereignisse, welche für die Abwicklung der Zusammenarbeit von Bedeutung sein können. Bei ausserordentlichen Ereignissen ist die andere Partei unverzüglich zu informieren.

## Verantwortlichkeiten Leistungsbezüger

Der Leistungsbezüger unterstützt den Leistungserbringer bei der Erfüllung seiner vertraglichen Pflichten mit seinen branchenspezifischen Kenntnissen und den notwendigen Informationen über seine dezentralen IT-Infrastrukturen. Er übermittelt ihm insbesondere betriebsrelevante Informationen rechtzeitig und vollständig.

Der Leistungsbezüger stellt u.a. für die Durchführung von Tests oder Leistungsabnahmen ausreichend Personal mit den notwendigen Qualifikationen zur Verfügung. Er unterstützt den Leistungserbringer namentlich auch bei der Analyse von Fehlern im Betrieb seiner Geschäftsanwendungen oder im Bereich seiner dezentralen IT-Infrastrukturen.

## Finanzielle Konditionen

Die Bearbeitung und Nutzung der besonders schützenswerten Personendaten und die Nutzung der Schnittstelle zu SVS Schulverwaltung (EdIS) ist für den Leistungserbringer kostenlos.

## Haftung

Der Leistungserbringer haftet dem Leistungsbezüger für den von ihm oder von einer seiner Hilfspersonen schuldhaft verursachten Schaden aus dem Vertragsverhältnis. Für absichtlich oder grobfahrlässig verursachten Schaden haftet sie unbeschränkt.

Bei leichter Fahrlässigkeit ist die Haftung des Leistungserbringers für Personenschäden unbegrenzt, für Sachschäden ist sie auf maximal Fr. 1'000'000 pro Fall und pro Rahmenvertrag beschränkt.

Der Leistungserbringer haftet - soweit gesetzlich zulässig - nicht für weitergehende oder andere Schäden, insbesondere nicht für indirekte Schäden oder Folgeschäden wie entgangener Gewinn, Verdienstausfall oder Ansprüche Dritter (wobei Organisationseinheiten des Leistungsbezügers, die vollständig unter seiner wirtschaftlichen Kontrolle sind, nicht als Dritte betrachtet werden).

Schadenereignisse sind zwecks Schadenminimierung der anderen Vertragspartei ohne Verzug zur Kenntnisnahme zu melden. Für Leistungen und Produkte von Dritten, welche der Leistungserbringer dem Leistungsbezüger vermittelt, gelten auch bezüglich Haftung ausschliesslich die Konditionen und Haftungsbestimmungen dieser Dritten. Für Subunternehmer und Hilfspersonen, die auf ausdrücklichen Wunsch des Leistungsbezügers beizuziehen sind, übernimmt der Leistungserbringer keine Haftung.

# Datenschutz

## Gesetzlicher Vertragsvorbehalt

Werden Personendaten durch Dritte bearbeitet, ist der Datenschutz gemäss § 12 Abs. 1 des Gesetzes über den Datenschutz des Kantons Thurgau (TG DSG) durch Vertrag oder Verfügung sicherzustellen. Zudem bestimmt § 13 TG DSG, dass bei der Bearbeitung von Personendaten für eine angemessene Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung oder Kenntnisnahme zu sorgen ist. Es ist daher zwischen dem Leistungsbezüger als öffentlichem Organ und dem Leistungserbringer als Drittem klarzustellen, unter welchen Voraussetzungen die dem Leistungserbringer zukommenden Daten bearbeitet werden dürfen. Als Bearbeitung wird jeder Umgang mit Daten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten verstanden.

## Datenherr

Der Leistungsbezüger behält die vollumfängliche Verfügungsmacht über die Daten. Er ist Datenherr und kann dem Leistungserbringer jederzeit den Zugriff auf die bearbeiteten Informationen verbieten, die Daten unentgeltlich in einem strukturierten, gängigen und maschinenlesbaren Format heraus verlangen und bzw. oder den Leistungserbringer auffordern, die bearbeiteten Informationen zu vernichten. Der Leistungserbringer ist nur im Rahmen der vertraglichen Vereinbarung berechtigt, die Daten zu bearbeiten.

## Zweck

Der Leistungserbringer darf die Daten nur zum vertraglich festgelegten Zweck verwenden. Weitergehende Verwendungszwecke müssen vom Leistungsbezüger vorab schriftlich bewilligt werden.

## Datenzugriff durch ausländisches Recht

Die Bearbeitung der Daten des Leistungsbezügers hat in der Schweiz zu erfolgen. Der Leistungserbringer informiert den Leistungsbezüger über sämtliche möglichen weiteren Datenbearbeitungsorte. Das Bearbeiten von Daten ausserhalb der Schweiz darf ausschliesslich in einem Land mit angemessenem Datenschutzniveau erfolgen. Sowohl die Datenbearbeitung als auch der Leistungserbringer und allenfalls weitere beteiligte Unternehmen dürfen keinen Bezug zu einem Staat aufweisen, welcher dem US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) oder einem gleichartigen Gesetz unterliegt (staatliche Offenbarungs- und Ermittlungsbefugnisse). Der Leistungsbezüger hat einen entsprechenden Bezug zum Ausland schriftlich zu bewilligen. Entsprechende Änderungen in der ausländischen Gesetzgebung, welchen der Leistungserbringer unterstellt ist, meldet dieser unmittelbar und selbständig dem Leistungsbezüger.

Inhalt und Ort der Informationsbestände sowie weitere Anknüpfungspunkte an ausländische Rechtsordnungen sind aktuell zu dokumentieren. Der Leistungserbringer stellt bei der Datenbearbeitung im Ausland sicher, dass Kontrollen durch die Behörden des Leistungsbezügers rechtlich zulässig und tatsächlich möglich sind.

## Informationsgesuche

Der Leistungserbringer informiert den Leistungsbezüger unverzüglich über alle bei diesem eingehenden Gesuche um Informationen zu den Daten. Er trifft organisatorische und technische Massnahmen, um dem Leistungsbezüger die Durchsetzung von datenschutzrechtlichen Ansprüchen, wie beispielsweise Löschungs- und Berichtigungsansprüche, zu ermöglichen. Der Leistungserbringer ist ohne Zustimmung des Leistungsbezügers nicht berechtigt, allfälligen Berichtigungs- oder Löschungsgesuchen Dritter direkt nachzukommen.

## Geheimhaltung

Die Bekanntgabe von Informationen an Dritte erfolgt ausschliesslich im Rahmen der vertraglichen Vereinbarung oder nach schriftlicher Ermächtigung des Leistungsbezügers. Die Pflicht zur Vertraulichkeit beinhaltet auch das Verbot der Einsichtsgewährung in Unterlagen und deren Herausgabe an Dritte sowie das Verbot des Kopierens von Informationen oder Informationsträgern zu persönlichen Zwecken. Nicht mehr benötigte Unterlagen und Kopien sind umgehend zu vernichten. Die Pflicht zur Vertraulichkeit ist den eigenen Mitarbeitern und anderen Hilfspersonen schriftlich aufzuerlegen. Sie entsteht schon vor Vertragsabschluss und bleibt auch nach der Beendigung dieses Vertrages bestehen. Der Leistungserbringer prüft die Hintergrundinformationen der neu eintretenden Mitarbeiterinnen und Mitarbeiter. Dies ist mindestens für Personen, die Zugriff auf ICT-Systeme der Leistungserbringung und die Kundendaten haben, erforderlich. Die Mitarbeiterinnen und Mitarbeiter des Leistungserbringers sind regelmässig auf die Themen Datenschutz und Informationssicherheit, insbesondere zur Geheimhaltung, zu sensibilisieren.

Sollte der Leistungserbringer aufgrund einer richterlichen Anordnung verpflichtet werden, an weitere Behörden oder an Dritte Zugang zu den Daten des Leistungsbezügers zu verschaffen, informiert er diesen unverzüglich. Der Leistungserbringer, dessen Mitarbeitende, Unterauftragnehmer und Hilfspersonen unterstehen im Rahmen der Vertragserfüllung der umfassenden Geheimhaltungs- und Schweigepflicht bzw. dem Amtsgeheimnis. Vorbehalten bleiben weitergehende gesetzlich verankerte Schweigepflichten (beispielsweise Berufsgeheimnisse). Diese Geheimhaltungspflichten beziehen sich auf alle Systeme, Prozesse und Informationen des Leistungserbringers und gelten auch innerhalb des Unternehmens des Leistungserbringers, ungeachtet der hierarchischen Positionen.

## Kontrollrecht

Der Leistungserbringer untersteht der Aufsicht der Kontrollorgane des Leistungsbezügers, namentlich der oder dem Datenschutzbeauftragten oder der Finanzkontrolle. Mitarbeitende des Leistungserbringers, des Unterauftragnehmers und Hilfspersonen unterstehen betreffend Datenbearbeitung ebenso dem Kontroll- und Weisungsrecht des Leistungsbezügers bzw. durch dessen Kontrollorgane. Der Leistungserbringer hat den Kontrollorganen des öffentlichen Organs Zugang zu dessen Informationen, Systemen und Prozessen zu verschaffen, die Kontrollorgane zu unterstützen sowie die zur Kontrolle notwendigen zeitlichen und fachlichen Ressourcen zur Verfügung zu stellen. Alle hier aufgeführten Dienstleistungen erfolgen unentgeltlich.

## Private Ansprüche

Datenschutzrechtliche Ansprüche werden beim Leistungserbringer und Serverbetreiber umgehend durchgesetzt. Dies beinhaltet Löschungs- und Berichtigungsrechte und erfolgt in Absprache mit dem Leistungsbezüger.

## Abgrenzung der Datenbearbeitung

Der Leistungserbringer trifft die notwendigen organisatorischen und technischen Massnahmen, um die Informationen des öffentlichen Organs von denjenigen anderer Leistungsbezüger zu trennen.

## Unterauftragsverhältnisse

Der Leistungserbringer darf Dritte zur Erfüllung seiner Aufgaben nur beiziehen, wenn ihm dies durch den Leistungsbezüger schriftlich bewilligt wurde. Der Unterauftragnehmer muss sämtliche Pflichten aus den

Vertragsverhältnissen zwischen dem Leistungsbezüger und dem Leistungserbringer sowie aus diesen Vertragseckwerten rechtsgültig übernehmen.

## Entwicklung und Wartung von Systemen

Erfordert die Entwicklung und Wartung von Systemen den Beizug Dritter, verhindert der Leistungserbringer durch organisatorische und technische Massnahmen, dass den Dritten Informationen des Leistungsbezügers zur Kenntnis gelangen. Lässt sich dies organisatorisch und technisch

nicht verhindern, dürfen Dritte nur mit schriftlicher Zustimmung des Leistungsbezügers beigezogen werden. Die beigezogenen Dritten müssen alle Pflichten aus den Vertragsverhältnissen zwischen dem Leistungsbezüger und dem Leistungserbringer sowie aus diesen Vertragseckwerten rechtsgültig übernehmen.

## Transparenz über Massnahmen

Der Leistungserbringer verpflichtet sich, den Leistungsbezüger spätestens innert 48 Stunden über besondere Vorkommnisse wie Datenverlust, Attacken, unrechtmässige Zugriffe, Zugriffsbeschränkungen, Ausfälle usw. zu informieren. Es sind formale Meldeverfahren mit aktuellen Ansprechadressen festzulegen.

## Sanktionen

Bei schwerwiegender Verletzung einer Bestimmung der vorliegenden Bestimmungen bezahlt der Leistungserbringer dem Leistungsbezüger eine Konventionalstrafe, sofern er nicht beweist, dass ihn kein Verschulden trifft. Die Höhe richtet sich nach der vertraglichen Vereinbarung, beträgt jedoch mindestens Fr. 50'000.-. Vorbehalten bleibt der Ersatz des darüber hinaus gehenden Schadens. Bei wiederholter Verletzung steht dem Leistungsbezüger das Recht zur sofortigen Vertragsauflösung zu. Der daraus entstehende Schaden ist ihm zu vergüten.

## Datenvernichtung

Der Leistungsbezüger kann vom Leistungserbringer während und nach der Vertragslaufzeit jederzeit die unentgeltliche Vernichtung von bearbeiteten Daten verlangen. Der Leistungserbringer verpflichtet sich, allfällige Kontrollen zur Löschung von Daten bzw. deren Löschung auch nach Beendigung des Vertrages zuzulassen.

## Datenportabilität

Der Leistungserbringer verpflichtet sich, dem Leistungsbezüger bei Auflösung des Vertrages alle bearbeiteten Daten umgehend und unentgeltlich in einem strukturierten, gängigen und maschinenlesbaren Format herauszugeben und diese anschliessend in Absprache mit dem Leistungsbezüger bei sich und bei allen beigezogenen Dritten zu vernichten bzw. vernichten zu lassen. Diese Pflichten können vom Leistungserbringer selbst dann nicht aufgeschoben werden, wenn zwischen den Parteien verschiedene Ansichten jeglicher Art über die Vertragserfüllung bestehen. Der Leistungserbringer hat somit die Datenportabilität und Interoperabilität bei Vertragsauflösung sicherzustellen.

Für den Fall, dass der Leistungsbezüger ihm gehörende IT-Geräte oder Softwarelizenzen des Leistungserbringers zum Betrieb übergeben hat, gibt der Leistungserbringer bei Beendigung der Zusammenarbeit die betreffenden IT-Geräte und Softwarelizenzen dem Leistungsbezüger zurück (Erfüllungsort Frauenfeld). Weitere Unterstützung des Leistungsbezügers durch den Leistungserbringer während des Ausstiegsprojekts kann gegen entsprechendes Entgelt vereinbart werden. Der Leistungserbringer ist jedoch nicht dazu verpflichtet, eigenes Know-How an den Leistungsbezüger oder Dritte weiter zu geben.

# Sicherheit

Der Leistungserbringer verpflichtet sich, die folgenden Massnahmen umzusetzen:

## ISO 27001

Der Leistungserbringer beachtet die Informationssicherheit gesamtheitlich in Anlehnung an ISO 27001.

## Anforderungskatalog C5

Die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten Massnahmen zur sicheren Cloudleistungserbringung gemäss dem BSI Standard Anforderungskatalog Cloud Computing (C5) (Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten) ist für die Leistungserbringung nachweislich zu berücksichtigen.

## Sicherheitsaktualisierung

Die Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Bedrohungen und Risiken werden mindestens jährlich durchlaufen, um Veränderungen und neue Einflussfaktoren zu berücksichtigen.

## Datenschutzaktualisierung

Der Leistungserbringer identifiziert mindestens jährlich die anzuwendenden gesetzlichen, vertraglichen und datenschutzrechtlichen Anforderungen.

## Vorabkontrolle

Die Lösung des externen Dienstleisters muss mit den verarbeiteten Daten und inklusive vertraglichen Regelungen vom Datenschutzbeauftragten des Kantons Thurgau geprüft und freigegeben werden.

## Vorfall

Der Leistungserbringer ist verpflichtet, bei einem Informationssicherheitsvorfall eine vertraglich definierte Konventionalstrafe zu entrichten (siehe AGB SIK).

## Subunternehmen

In die Leistungserfüllung involvierte Drittunternehmen müssten dem Leistungsbezüger jederzeit bekannt sein und werden durch den Leistungserbringer in gleichem Masse verpflichtet, Datenschutz, Geheimhaltung und Informationssicherheit sowie Vertragsverpflichtungen zu erfüllen.

## Datenflussdokumentation

Die Lösung ist mit den Systemen, den Datenflüssen und der Datenverarbeitung zu dokumentieren. Dies umfasst ebenso die Örtlichkeit mitsamt Nennung des Landes, der Ortschaft und der Anschrift des Rechenzentrums und des Betreibers mitsamt der Nennung von dessen Zertifizierungen.

## Schutzmassnahmen

Es sind Massnahmen implementiert, um die Daten und den Service vor unerwünschten Ereignissen zu schützen. Dies nach dem Credo die Daten müssen gemäss jeweiligem aktuellen Stand der Technik bestmöglich geschützt werden.

## Best Practice

Die Systeme müssen nach Best Practice gehärtet sein und haben dadurch entsprechend hohe Schutzbedarfsanforderungen zu erfüllen.

## Schwachstellenmanagement

Für sämtliche Systeme ist ein Schwachstellenmanagement im Einsatz. Aktuelle Bedrohungen werden detektiert, beurteilt und zeitnahe Massnahmen zur Eliminierung der Schwachstellen werden implementiert. Sogenannte Zero Days sind innert 48 Stunden nach Veröffentlichung eines Patches oder einer Massnahme des Herstellers geschlossen oder zumindest die Auswirkungen minimiert.

## Logdateien

Die Logs der Systeme sind zu überwachen. Ereignisse werden beurteilt und zeitnah als Massnahmen umzusetzen.

## Malwareschutz

Die involvierten Assets sind durch einen aktuellen und nach heutigem Stand der Technik implementierten Malwareschutz zu sichern.

## Zuordnung

Aktionen wie Authentisierung, Autorisation, Zugriff, Änderungen etc. sind eindeutig Kunden sowie identifizierbaren Benutzern oder personalisierten Systemadministratoren zugeordnet. Diese Logs sind revisionssicher zu speichern.

## Private Schlüssel

Bei verschlüsselten Daten ist sicherzustellen, dass ausschliesslich der Leistungsbezüger im Besitze der privaten Schlüssel ist. Ein Konzept liegt vor.

## Datentransfer

Datentransfers sind durch eine sichere und aktuelle Transportverschlüsselung (TLS) mit sicheren kryptografischen Algorithmen gesichert (siehe BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen).

## Zugriffsbeschränkung

Die Schnittstelle zum Kanton Thurgau, wie auch andere externe Schnittstellen, haben eine zertifikatsbasierte Authentisierung (Mutual Authentication oder auch Two-Way SSL Authentication) implementiert. Zusätzlich ist eine IP zu IP Freischaltung (Webserver zu Webserver) mit dem spezifizierten Port und Protokoll konfiguriert. Interne Schnittstellen haben eine wirksame Authentisierung und eine Zugriffsbeschränkung.

## Datenaustausch

Es sind Massnahmen implementiert, um die Integrität beim Export sowie Import aller beteiligten Systeme zu gewährleisten.

## Identity und Access Management

Das Identity und Access Management (IAM) ist dokumentiert und sicher implementiert. Das IAM regelt die Zugriffsbereitstellung, das Änderungsmanagement, die Passwortrichtlinie, sichere Anmeldeverfahren und die Zwei-Faktoren-Authentisierung. Die Passwortrichtlinie entspricht dem Stand der Technik für ein sicheres Passwort. Mehrere Falschanmeldungen werden detektiert und haben eine zeitlich beschränkte Sperrung zur Folge.

## Zwei-Faktor-Authentisierung

Der Zugriff auf die Lösung und die Daten, erfolgt ausschliesslich mittels Zwei-Faktor-Authentisierung. Dies gilt auch beim Einsatz von Apps auf einem mobilen Device. Ausgenommen sind Zugriffe auf öffentliche Informationen, soweit keine Personen bestimmt oder bestimmbar sind bzw. werden.

## Zertifikate

Für Benutzerzugriffe auf Webapplikationen und Apps etc. werden ausschliesslich offizielle SSL-Zertifikate eines vertrauenswürdigen Anbieters eingesetzt.

## Firewall

Netzwerkübergänge sind durch Firewalls mit einem wirksamen Regelset sowie einer Threat Prevention zu sichern.

## Benutzerüberwachung

Im Zusammenhang mit der Leistungserbringung werden keine externen Analyse-Tools wie Google-Analytics etc. eingesetzt. Es kommen auch keine externen Schriften oder externe Symbole, die cloudbasierend von externen Ressourcen eingebunden sind, zur Anwendung. Lokale Analysen können für eigene Zwecke des Dateneigentümers oder Leistungserbringers angewendet werden. Die gesetzlichen Rahmenbedingungen sind einzuhalten.

## Zeitsynchronisation

Alle Assets, die in die Leistungserbringung involviert sind, sind mit einem zentralen Zeitserver zu synchronisieren.

## Kommunikation

Der Anbieter stellt die E-Mailkommunikation zur Verfügung und sichert den Transport mit einer aktuellen TLS-Version. Eine vom Kanton verwendete Domain steht für die E-Mailkommunikation nicht zur Verfügung. Die E-Mailserver des Netzwerkes des Kantons Thurgau stehen für den Versand von E-Mails für externe Dienste nicht zur Verfügung.

## Sicherheitstests

Der externe Leistungserbringer lässt die ICT-Lösung, welche die Daten der Schnittstelle verwendet, mittels Penetrationtests / Assessments periodisch überprüfen. Ein Nachweis kann der Leistungserbringer jederzeit erbringen.

## Physische Sicherheit

Für die Leistungserbringung sind angemessene Sicherheitsmassnahmen zum Schutz vor Bedrohungen von aussen und aus der Umgebung (physische Sicherheit) zu betreiben.

## Betriebskontinuität

Die Planung der Betriebskontinuität ist etabliert und die Verfahren betreffend ICT-Continuity mit Datensicherung, Wiederherstellung und Betrieb eines Ausweichstandortes sind nachweislich zu verifizieren.

# Schlussbestimmungen

## Vertragsdauer und Kündigung

Dieser Rahmenvertrag gilt auf unbestimmte Zeit. Er kann von jeder Partei unter Einhaltung einer Kündigungsfrist von sechs Monaten auf das Ende eines Jahres schriftlich gekündigt werden. Die Verpflichtung zur Vertraulichkeit bleibt über das Vertragsende hinaus bestehen

## Salvatorische Klausel

Änderungen und Ergänzungen dieses Rahmenvertrags, eines Einzelvertrages und seiner Anhänge bedürfen der Schriftform. Auf die Schriftform darf nur schriftlich verzichtet werden. Sollten sich einzelne Regelungen des Vertragswerks als rechtsunwirksam oder nicht durchführbar erweisen, werden die unwirksamen oder undurchführbaren Regelungen durch wirksame oder durchführbare Bestimmungen ersetzt, die dem bei Vereinbarung der jeweiligen Regelung vorhandenen Willen der Vertragsparteien wirtschaftlich am nächsten kommen. Die Wirksamkeit der übrigen Regelungen bzw. dieses Rahmenvertrags bleibt unberührt. Die vorstehende Regelung gilt entsprechend auch für den Fall, dass das Vertragswerk Lücken enthalten sollte.

## Anwendbares Recht und Gerichtsstand

Für allfällige Streitigkeiten aus diesem Vertragsverhältnis gilt der ordentliche Gerichtsstand des Leistungsbezügers. Der Leistungserbringer ist auch am eigenen Sitz bzw. Wohnsitz einklagbar. Anwendbar ist schweizerisches Recht, insbesondere die Datenschutzgesetzgebung des Kantons Thurgau sowie die AGB der Schweizerischen Informatikkonferenz (SIK) Ausgabe Januar 2020.

Mit den obigen Ausführungen erklären sich einverstanden:

**Unterschriften**

Ort, Datum: Ort, Datum:

Weinfelden, 6. April 2018

**Kanton Thurgau** xxx **xxx**

**Amt für Informatik**

Christoph Maier Vorname Name (Leistungserbringer)

Amtsleiter Titel