Selbstdeklaration des SaaS-Anbieters
zum Rahmenvertrag
für die Bereitstellung und den Betrieb
von ärztlichen Fachapplikationen aus der Cloud

---

1. Anbieterdaten

Die untenstehenden Angaben sind vollständig auszufüllen.

Deklaration	Angaben des Anbieters
1.1. UID-Nr. (www.zefix.ch)	
1.2. Firmenname und Rechtsform	
1.3. Strasse / Postfach	
1.4. PLZ / Ort Hauptsitz	
1.5. Weitere Unternehmensstandorte	
1.6. Name Kontaktperson	
1.7. Direkte Telefonnummer Kontaktperson	
1.8. Direkte E-Mailadresse Kontaktperson	
1.9. Sind Sie ein Anbieter mit Auslandsbezug (insbesondere Sitz, Muttergesellschaft, Tochtergesellschaften, Börsenkotierung im Ausland, Niederlassungen oder Rechenzentren im Ausland)?	☐ Ja ☐ Nein

2. Subunternehmer

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
2.1. Der Anbieter listet alle vorgesehenen Subunternehmer mit ihren Namen, den von ihnen erbrachten Leistungen und dem Ort der Leistungserbringung auf.		
2.2. Der Anbieter bestätigt, dass er zur Kenntnis genommen hat, dass er bei falschen oder unvollständigen Auskünften und/oder Angaben für die sich daraus ergebenden Folgen einzustehen hat.		

3. Akzept des Rahmenvertrages und Auslandbezug

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
3.1. Der Anbieter akzeptiert den Rahmen-vertrag für Cloudservices der FMH als verbindliche Vertragsgrundlage.		
3.2. Der Anbieter erbringt seine Leistungen aus diesem Rahmenvertrag gegenüber dem Kunden ausschliesslich in der Schweiz. Insbesondere finden sämtliche Datenbearbeitungsvorgänge (inkl. Betrieb von Applikations-servern) ausschliesslich in der Schweiz statt.		
3.3. Der Anbieter bestätigt, dass sämtliche Leistungen unter dem Rahmenvertrag der FMH ausschliesslich schweizerischem Recht unterstehen (Ziffer 5.13. Rahmenvertrag).		
3.4. Der Anbieter bestätigt, dass weder er noch eines seiner Subunternehmen einem ausländischen Recht untersteht, das ausländischen Behörden einen Anspruch auf Herausgabe von Kundendaten einräumt.		
3.5. Für Anbieter mit Auslandbezug: Der Anbieter listet alle Standorte seiner Konzerngesellschaften (Mutter/Töchter) und Niederlassungen im Ausland, seiner Rechenzentren, in denen Daten des Kunden gespeichert werden können und der Orte, von denen aus ein Zugriff auf Daten und Systeme des Kunden möglich sind (z.B. im Rahmen des Supports und der Wartung), auf.		

3.6. Besteht eine Kotierung des Anbieters oder einer zum Konzern des Anbieters gehörenden Gesellschaft an einer ausländischen Börse? Wenn ja, um welche Gesellschaft(en) handelt es sich und an welcher Börse ist/sind diese kotiert?		

4. Organisatorische Massnahmen

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
4.1. Der Anbieter stellt dem Kunden eine umfassende Dokumentation zu allen angebotenen SaaS-Dienstleistungen zur Verfügung, welche alle enthaltenen Funktionen beschreibt und umfassend über deren Verwendung informiert.		
4.2. Setzt der Anbieter Software von Drittanbietern ein? Wenn ja welche?		
4.3. Muss allfällige Software von Drittanbietern durch separate zusätzliche Lizenz- und/oder Wartungsverträge abgesichert werden?		
4.4. Verfügt der Anbieter über die erforderlichen Nutzungs- und Vertriebsrechte an der eingesetzten Software von Drittanbietern?		
4.5. Wie stellt der Anbieter dem Kunden bei einem Ausfall des Cloudservice von mehr als 2 Werktagen konkret eine Umgehungslösung für die Sicherstellung eines fortlaufenden operativen Betriebs zur Verfügung (Ziffer 3.6. Rahmenvertrag)?		
4.6. Wie verpflichtet der Anbieter konkret seine Mitarbeitenden zur Geheimhaltung (Ziffer 5.2. Rahmenvertrag)?		
4.7. Wie verpflichtet der Anbieter konkret seine Mitarbeitenden zur Einhaltung der betrieblichen, technischen und sicherheitsrelevanten Vorschriften des Kunden (Ziffer 5.3. Rahmenvertrag)?		
4.8. Gibt der Anbieter eine ausdrückliche schriftliche Erklärung bezüglich der Einhaltung der Datenschutz- und Datensicherheits-bestimmungen gegenüber dem Kunden ab (Ziffer 5.4. Rahmenvertrag)? Wenn ja, wo und mit welchem Inhalt?		

4.9. Legt der Anbieter eine Vertraulichkeits-vereinbarung für alle involvierten Mitarbeitenden gegenüber dem Kunden vor (Ziffer 5.4. Rahmenvertrag)?		
4.10. Legt der Anbieter eine Vertraulichkeits-vereinbarung mit allen beigezogenen Dritten (Subunternehmern) gegenüber dem Kunden vor (Ziffer 5.4. Rahmenvertrag)?		
4.11. Wie hat der Anbieter konkret seine innerbetriebliche Organisation ausgestaltet, damit er den besonderen Anforderungen des Datenschutzes gerecht werden kann (Ziffer 5.5. Rahmenvertrag)?		
4.12. Legt der Anbieter dem Kunden einen Raster zur Erarbeitung der Datenschutz-Folgeabschätzung (Risikomatrix, Massnahmenkatalog) vor?		
4.13. Bestätigt der Anbieter gegenüber dem Kunden, dass er als Datenverarbeiter in der gleichen Verantwortung steht wie der Kunde, der als Verantwortlicher für die Patientendaten einzustehen hat? Wenn ja, wo und mit welchem Inhalt?		
4.14. Bietet der Anbieter dem Kunden ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der eingesetzten technischen und organisatorischen Massnahmen (Ziffer 5.8. Rahmenvertrag)? Wie sieht dieses Verfahren konkret aus?		
4.15. Bietet der Anbieter dem Kunden ein dokumentiertes Verfahren an, welches sicherstellt, dass dem Kunden innerhalb von 72 Stunden nach Kenntnisnahme einer Datenschutzverletzung umgehend und umfassend Bericht erstattet wird? Wie sieht dieses Verfahren konkret aus?		
4.17. Kann der Anbieter dem Kunden schriftliche Überbindungsverträge an Subunternehmer vorlegen, in welchen diese in die gesamten Pflichten aus dem Rahmenvertrag und den Datenschutzauflagen eingebunden werden (Ziffer 5.5. Rahmenvertrag)?		

4.18. Wie sieht das vom Anbieter dem Kunden gegenüber zu gewährende Auditrecht a. für ihn selber b. für die beigezogenen Dritten (Ziffer 5.10 Rahmenvertrag) konkret aus?		
4.19. Legt der Anbieter dem Kunden die mit der Serviceerbringung betrauten Personen namentlich offen (Ziffer 5. 11 Rahmenvertrag)? Wie sieht diese Offenlegung konkret aus?		
4.20 Überbindet der Anbieter den mit der Serviceerbringung betrauten Personen die Strafbestimmungen bezüglich der Wahrung des Arztgeheimnisses (Art. 321 StGB) in schriftlicher Form (Ziffer 5.11. Rahmenvertrag)? Wie sieht diese Überbindungserklärung konkret aus?		
4.21. Wie stellt der Anbieter gegenüber dem Kunden konkret sicher, dass die mit der Serviceerbringung betrauten Personen jederzeit über einen einwandfreien Leumund verfügen (Ziffer 5.11 Rahmenvertrag)?		
4.22. Wie räumt der Anbieter dem Kunden das Kontrollrecht bezüglich der Einhaltung der gesetzlichen Bestimmungen, der vertraglichen Bestimmungen, der SLA und der Selbst-deklaration konkret ein (Ziffer 5.13 und 5.14 Rahmenvertrag)?		
4.23. Wie stellt der Anbieter sicher, dass ohne ausdrückliches Einverständnis des Kunden nicht mit seinem Namen oder seiner Praxisbezeichnung Werbung in Bezug auf das Vertragsverhältnis betrieben wird (Ziffer 5.16 Rahmenvertrag)?		
4.24. Der Anbieter zeigt auf, wie er sofort alle Umstände gegenüber dem Kunden anzeigt, welche die vertragsgemässe Erfüllung gefährden oder gefährden könnten (Ziffer 6.3 Rahmenvertrag).		
4.25. Der Anbieter zeigt dem Kunden auf, wie er über Verbesserungen und Weiterentwick-lungen, die eine Veränderung der Leistungen angezeigt erscheinen lassen, konkret orientieren wird (Ziffer 7.1. Rahmenvertrag).		

4.26. Der Anbieter zeigt dem Kunden auf, welche Leistungen er bezüglich folgender Leistungsbereiche im Einzelnen zum angebotenen Preis abdeckt: a. Wartung b. Pflege c. Support d. Weiterentwicklung		
4.27. Der Anbieter zeigt dem Kunden konkret auf, wie er den Qualitätsreview bezüglich seiner Leistungen konkret durchführt (Ziffer 12.2. Rahmenvertrag)?		
4.28. Unterhält der Anbieter eine Meldestelle für Praxismitarbeitende bei einem Sicherheits-vorfall? Wie lautet diese konkret? Hat der Anbieter eine Prozessbeschreibung dazu?		
4.29. Ist eine Kontaktperson für die Meldung von Sicherheitsvorfällen sowie eine Stellvertretung festgelegt? Sind die Kontaktangaben und die Erreichbarkeit der Meldestelle den Praxismitarbeitenden bekannt gemacht?		
4.30. Verfügt der Anbieter über Merkblätter für Praxismitarbeitende zum Vorgehen bei einem Sicherheitsvorfall? Wie lauten diese Merkblätter konkret?		
4.31. Welche konkreten periodischen Rapporte und Informationen bietet der Anbieter dem Kunden in Bezug auf das gesamte vertragliche Leistungsangebot?		
4.32. Unterstützt der Anbieter den Kunden mit konkreten Empfehlungen und praxis-orientierten Sicherheitsvorgaben im Zusammenhang mit der Anbindung an die Cloud-Applikationen? Wie sehen diese konkret aus?		
4.33. Führt der Anbieter regelmässig Kontrollen nach internationalen Audit-Standards durch? Stellt der Anbieter die Prüfungsresultate unabhängiger Kontrollstellen dem öffentlichen Organ zur Verfügung?		

4.34. Trennt der Anbieter in seiner IT-Infrastruktur (Server, Datenbanken, Netzwerk etc.) die Patientendaten von übrigen Datendurch entsprechende Segmentierung (resp. Zonierung)? Wenn ja, wie sieht das konkret bei ihm aus? Wenn nein, warum nicht?		

5. Technische Massnahmen

Die nachfolgenden Massnahmen sind insbesondere dem Leitfaden des Eidgenössischen Datenschutzbeauftragten für die Bearbeitung von Personendaten im medizinischen Bereich vom Juli 2002 sowie den Minimalanforderungen der FMH für IT-Grundschutz für Praxisärztinnen und Praxisärzte (https://www.fmh.ch/dienstleistungen/e-health/it-grundschutz.cfm) entnommen.

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
5.1. Erlässt der Anbieter zuhanden des Kunden konkrete Sicherheitsvorgaben, welche dieser umzusetzen und einzuhalten hat? Wenn ja, welche? Kann er dafür die entsprechenden Vorgaben vorlegen?		
5.2. Wie stellt der Anbieter konkret sicher, dass Zugriffe auf Applikationen, in welchen Personendaten bearbeitet werden, protokolliert werden (Ziffer 5.12. Rahmenvertrag)? Wie sehen die konkreten Überwachungsdaten aus, die der Anbieter dem Kunden zur Verfügung stellen kann?		
5.3. Der Anbieter zeigt auf, welche anerkannten Methoden und aktuellen Standards er im Zusammenhang mit der vertragsgemässen Erfüllung im Bereich Datenschutz und Datensicherheit konkret anwendet (Ziffer 6.4 Rahmenvertrag)?		
5.4. Wie stellt der Anbieter konkret sicher, dass nur berechtigte Personen auf die Patientendaten Zugriff erhalten (Berechtigungskonzept, Log über Zugriffe, Benutzerkonto, starke Authentisierungen beim Zugriff über Internet etc.)?		

5.5. Bietet der Anbieter eine Authentisierung der Zugriffsberechtigten über eine HIN-Identität oder andere Authentisierungsmechanismen für den Zugriff auf die Applikationen in der Cloud an (z.B. Zweifaktorauthentisierung, Token etc.)?		
5.6. Setzt der Anbieter Erkennungsmechanismen ein, welche atypisches Verhalten bei den Benutzerkonten oder bei der Benutzung der Applikationen in der Cloud (z.B. Log-in und Log-out, function alerts etc.) feststellen können? Wenn ja, welche konkret?		
5.7. Wird der Zugriff über das Internet auf die Cloud-Applikation(en) durch einen besonders verschlüsselten Kanal (VPN oder HTTPS) sichergestellt? Welche Zugriffsmethoden bietet der Anbieter konkret an?		
5.8. Mit welchen technischen Mitteln stellt der Anbieter sicher, dass die Nachvollziehbarkeit der Datenbearbeitung in seinen Applikationen in der Cloud jederzeit sichergestellt ist und Aufzeichnungen jederzeit reproduzierbar sind?		
5.9. Lässt der Anbieter seine IT-Infrastrukturen, auf welchen die Fachapplikationen für die Ärztinnen und Ärzte in der Cloud abgewickelt werden, regelmässig durch Dritte überprüfen? Wenn ja, wie konkret? Kann der Anbieter solche Prüfungsab-klärungen konkret vorweisen?		
5.10. Bietet der Anbieter dem Kunden Sicherheitsvorkehrungen bei den Schnittstellen und Komponenten zum Internet (Firewalls) oder bei den kabelgebundenen und kabellosen Anschlüssen im lokalen Netzwerk an? Wenn ja, welche konkret? Kann der Anbieter solche Vorkehrungen konkret vorweisen?		

5.11. Bietet der Anbieter dem Kunden Konfigurationsvorlagen für seine Arbeitsplätze an, mit welchen der Kunde auf die Applikationen zugreift? Wenn ja, welche konkret? Kann der Anbieter solche Vorlagen konkret vorweisen?		
5.12. Definiert der Anbieter gegenüber dem Kunden spezielle Anforderungen für die Einbindung von Laborgeräten (z.B. Verschiebung in separate Netzwerkzonen) als Voraussetzung eines Cloudanschlusses? Wenn ja, welche konkreten Anforderungen?		
5.13. Verlangt der Anbieter gegenüber dem Kunden, dass er seine ICT-Systeme (z.B. seine Arbeitsplätze in der Praxis) mit verschiedenen Massnahmen besonders «härtet», bevor ihm Zugriff auf die Cloud-Applikationen gewährt wird (z.B. automatische Installation von Sicherheitsupdates, Zugriff über HIN-ID, Verschlüsselung der Festplatten, Verwendung besonders gesicherte Passworte, Endpoint Security von HIN, Alarmierungen etc.)? Wenn ja, welche konkreten Massnahmen?		
5.14. Bietet der Anbieter in Bezug auf alle Daten in der Cloud-Applikation eine eigene Datensicherung an? Wenn ja, wie sieht diese konkret aus? Werden die Backup-Daten verschlüsselt übermittelt und verschlüsselt abgelegt? Wohin werden die Daten gesichert? Hat der Kunde Zugriff auf diese Backups?		
5.15. Sind die Daten in der Transport- und Speicherphase während der Ver- und Entschlüsselung sowie während der Verarbeitung geschützt und vor einem unberechtigten Zugriff aus dem Netzwerk des Cloud-Anbieters sicher? Wenn ja, welche Methode wird angewendet?		
5.16. Bietet der Anbieter dem Kunden eine periodische Überprüfung resp. Wiederherstellung der erstellten Backups an (Restore-Prozeduren)? Wenn ja, wie sieht diese konkret aus? Was hat der Kunde diesbezüglich vorzukehren und an Leistungen zu erbringen?		

5.17. Ist der Kunde verpflichtet, eine eigene Datensicherung zu installieren? Wenn ja, welche Voraussetzungen muss er diesbezüglich erfüllen? Wie stellt der Anbieter sicher, dass solche persönlichen Datensicherungen wieder in die Cloud-Applikation eingespielt werden können?		
5.18. Welche technischen Massnahmen kehrt der Anbieter vor, um gemäss Art. 8 der Datenschutz-Verordnung der Schweiz folgende Risiken bezüglich der Patientendaten abzudecken: a. unbefugte und zufällige Vernichtung; b. zufälliger Verlust; c. technische Fehler; d. Fälschung, Diebstahl oder widerrechtliche Verwendung; e. unbefugtes, Ändern, Kopieren, Zugriffe oder andere unbefugte Bearbeitungen. Wie sehen die Massnahmen konkret aus?		
5.19. Welche konkreten technischen Massnahmen ergreift der Anbieter, um seine ICT-Cloud-Infrastrukturen (Server, Applikationen, Netzwerkkomponenten etc.) in Bezug auf Befall mit Schadsoftware (Viren, Würmer, Trojaner) zeitnah zu erkennen und möglichst auszuschliessen?		
5.20. Sind vom Anbieter alle eingesetzten ICT-Systeme (beispielsweise Server, Netzwerkkomponenten, Datenträger sowie Anwendungen mit zuvor festgelegten Attributen in einem Inventar erfasst worden? • Kann der Anbieter dem Kunden diese Inventarisierung (unter Wahrung der Geschäftsgeheimnisse) zeigen.		

Der Anbieter bestätigt mit seiner Unterschrift, dass die Angaben in dieser Selbstdeklaration richtig und vollständig sind. Der Anbieter nimmt zur Kenntnis, dass mit seiner Unterschrift diese Selbstdeklaration integrierender Bestandteil des Rahmenvertrages (vgl. Ziffer 2.1. Rahmenvertrag) wird und den Anbieter zur Einhaltung der wiedergegebenen Massnahmen, Aktivitäten oder Handlungen verpflichtet.

Ort / Datum:

.....

Rechtsverbindliche Unterschriften des Anbieters:

.....

.....