ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Die Kommission

Chorherrengasse 2, 1700 Freiburg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/odsb

Freiburg, 28. August 2017

Merkblatt über die Auslagerung der Datenbearbeitung des Staates Freiburg in eine Cloud
—
2017-PrD-77

I. Einleitung

Das Hosting der E-Mail-Anwendung Outlook macht nur einen kleinen Teil der Auslagerungsnachfrage aus. Tatsächlich sind mehrere Anfragen verschiedener Mitarbeitender des Amts für Informatik und Telekommunikation (ITA) bei unserer Behörde eingegangen. Sie beziehen sich namentlich auf das neue Steuerregister, die Weiterentwicklung der Informatikplattform FRI-PERS, die Auslagerung des Hostings, des Betriebs und Unterhalts der Websites des Kantons Freiburg, die Verwaltung der Mobilapparate sowie die Einführung von Office 365 und Skype for business.

Um dem ITA eine Orientierungshilfe für die verschiedenen laufenden und künftigen Projekte zu geben, gehen wir hier auf die Auslagerung der Datenbearbeitung öffentlicher Organe in Clouds im Allgemeinen ein. Unsere Analyse lehnt sich zudem an die Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und das Merkblatt von PRIVATIM zum Cloud Computing im Schulbereich an.

II. Risiken bei Auslagerung[1]

A. Risiken hinsichtlich Verlust der Kontrolle über das eigene IT-System

Wegen der weltweiten Vernetzung und der Virtualität ist der Standort der Daten oft nicht erkennbar. Dies trifft im besonderen Mass für die Public Clouds zu. Der Cloud-Nutzer als verantwortlicher Dateninhaber weiss damit nicht, wo genau seine Daten in der Cloud gespeichert und verarbeitet werden. Er weiss oft auch nicht, ob Subunternehmer involviert sind und ob diese für einen angemessenen Datenschutz sorgen. Der Cloud-Nutzer kann somit seine datenschutzrechtlichen Pflichten hinsichtlich Gewährleistung der Datensicherheit, Gewährung des Auskunftsrechts oder Berichtigung und Löschung der Daten nicht (mehr) oder nur ungenügend wahrnehmen.

Risiken bestehen hinsichtlich:

> **Unterauftragsverhältnis**: Es muss geprüft werden, ob der Subunternehmer über die für die Leistungserbringung notwendigen technischen und finanziellen Kapazitäten verfügt; es ist dafür zu sorgen, dass bei Unterauftragsvergabe die vom Auftraggeber vorgegebenen

[1] EDÖB, Erläuterungen zu Cloud Computing (https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de); Guide de l'externalisation des systèmes d'information de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2010 (http://www.ssi.gouv.fr/externalisation).

Sicherheitsanforderungen nicht ausgehebelt werden; der Auftraggeber muss sich das Recht vorbehalten, jeden Unterauftrag ohne ausreichende Garantien zur Leistungserfüllung entsprechend den Sicherheitsanforderungen zurückzuziehen; jegliches Bearbeiten von Daten durch einen Subunternehmer darf nur nach den Weisungen des Verantwortlichen für die Datenbearbeitung erfolgen und unter der Voraussetzung, dass Datensicherheit und Vertraulichkeit vertraglich garantiert sind.

> **Datenlokalisierung**: Es kann vorkommen, dass Teile eines Datensatzes in verschiedenen weltweit verstreuten Rechenzentren liegen; deshalb muss sichergestellt werden, dass die Sicherheitsanforderungen erfüllt und die gesetzlichen Vorschriften eingehalten sind, wo immer die Daten gehostet werden (angemessenes Datenschutzniveau des Staates). Die verstreuten Datenstandorte sind nicht nur in Bezug auf die Gewährleistung von Datenschutz und Datensicherheit problematisch, sondern auch in Bezug auf die Einhaltung von anderen gesetzlichen Pflichten (Aufbewahrungspflicht, Auskunftsrecht, Einhaltung von Geheimhaltungspflichten, Audit, usw.).

> **Zugriff von ausländischen Behörden auf die Daten:** In vielen Fällen werden die Daten für die Bearbeitung in der Cloud ins Ausland bekannt gegeben. Dabei werden die Daten oftmals auch in Ländern gespeichert oder bearbeitet, die über keinen (ausreichenden) Datenschutz verfügen. Cloud-Service-Anbieter sind aber auch gegenüber ausländischen Behörden und Gerichten verpflichtet, gegebenenfalls Zugriff auf Daten in der Cloud zu gewähren; dies gilt selbst dann, wenn die Daten nicht im Land der Behörde bearbeitet oder gespeichert werden.

> **Lock-in Effekte:** Ein weiteres Risiko ist die Abhängigkeit vom Cloud-Service-Anbieter und fehlende Portabilität und Interoperabilität. Das heisst, die Daten können wegen nicht vorhandener standardisierter Technologien und Schnittstellen nicht (mehr) oder nur mit grossem finanziellen und/oder technischem Aufwand ins eigene IT-System zurückgeführt oder zu einem anderen Cloud-Anbieter migriert werden.

> **Datenverlust**: Daten können durch Diebstahl, Löschung, fehlerhafte Überschreibung oder sonstige Veränderung verloren gehen. So müssen unbedingt Backup-Systeme für die Originaldaten und entsprechende Sicherheitssysteme implementiert werden.

> **System- und Netzwerkausfälle sowie Nichtverfügbarkeit angemieteter Ressourcen und Services** können dazu führen, dass Daten verloren gehen oder unberechtigten Personen zugänglich werden und dass damit die Vertraulichkeit, Sicherheit und Integrität der Daten nicht mehr gewährleistet ist. Überdies können solche Ausfälle den Geschäftsbetrieb eines Unternehmens oder der Behörde massiv beeinträchtigen und nebst finanziellen Verlusten auch gravierende Reputationsschäden nach sich ziehen.

> **Missbrauch der Daten**: Bei einem Outsourcing legt der Service-Anbieter unter Umständen nicht offen, wie die Zugriffsberechtigungen (physisch und virtuell) seiner Mitarbeitenden geregelt sind und wie diese diesbezüglich überwacht werden. Auch die Vertraulichkeits-erklärungen sind für den Nutzer oft nicht einsehbar. Im Bereich Cloud Computing muss diesem Problem umso mehr Aufmerksamkeit gewidmet werden, wenn es um eine Public Cloud geht.

B. Risiken bei Fernsupport

Outsourcing setzt oft Fernzugriffsverbindungen voraus. Dadurch, dass es keine Vor-Ort-Einsätze von Technikern braucht, lässt sich mit Fernwartung viel Zeit und Geld sparen. Die Fernwartung kann aber je nachdem auch Angriffsflächen eröffnen: permanente externe Verbindung, Standard-

Passwörter (allgemein bekannt) oder schwache Passwörter, Schwachstellen bei den Zugangs-Schnittstellen, Fernwartungs-Betriebssysteme, die nicht auf den neusten Stand sind, keine Rückverfolgbarkeit der Tätigkeiten, Verantwortliche und Mitarbeitende ohne Bewusstsein für Sicherheitsprobleme oder schlecht ausgebildet, Vernetzung gesicherter Systeme mit Systemen mit geringerem Sicherheitsniveau (z.B. Internet).

Die Risiken des Fernsupports sind:

> Eindringen Unbefugter in das IT-System: Ausfall des Computers oder des ganzen IT-Systems; Vertraulichkeit oder Integrität der Daten im IT-System nicht mehr gewährleistet;

> Missbrauch der Rechte eines Technikers des Supportcenters bei der Wartung: Zugriff auf vertrauliche Daten oder Herunterladen solcher Daten im grossen Stil, Ändern von Daten, keine Rückverfolgbarkeit.

Es wird empfohlen, die Verbindung beispielsweise über VPN zu sichern, den Zugang mit Zugriffsrechten einzuschränken, eine Authentifizierungspflicht für die für den Support zuständigen Techniker vorzusehen, eine Rückverfolgbarkeit der Tätigkeiten zu gewährleisten, Audits durchzuführen und auch für die organisatorischen Massnahmen zu sorgen.

C. Risiken bei Shared Hosting

Dem Konzept von Cloud Computing ist inhärent, dass verschiedene Nutzer, die in keiner Beziehung zueinander stehen, ihre Daten in derselben Cloud und durch dasselbe System verarbeiten lassen. Damit erhöht sich das Risiko, durch Attacken auf einen der Nutzer in Mitleidenschaft gezogen zu werden. Die eigenen Daten könnten also wegen Hackerangriffen oder Distributed-Denial-of-Services-Attacken nicht mehr verfügbar sein oder selbst «mitgehackt» werden. Es ist deshalb eminent wichtig, dass die Datenbearbeitungen der verschiedenen Cloud-Nutzer strikt voneinander getrennt werden und es nicht zu einer Vermischung der Daten kommt.

So ist dem Hosting auf einem dedizierten Server der Vorzug zu geben. Entscheidet man sich für ein Shared Hosting, so sollte eingehend abgeklärt werden, was für Folgen alle potenziellen Attacken haben könnten, und vertraglich vereinbart werden, wie eine allfällige Störung wirksam behoben werden kann, insbesondere die Wiederherstellung sämtlicher Protokolldateien und die Trennung vom Netz, ohne Abschalten der betroffenen Rechner.

III. Nutzung von Cloud Computing-Diensten aus Sicht des Datenschutzes

Öffentliche Organe, die die Bearbeitung ihrer Daten in eine Cloud auslagern wollen, müssen die datenschutzrechtlichen Vorschriften einhalten:

> Nach Artikel 10 DSchG dürfen sie Personendaten nur dann Dritten bekanntgeben, wenn eine **gesetzliche Bestimmung es vorsieht** (systematische Bekanntgabe). Der Cloud-Service-Anbieter muss also verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer, die vom Anbieter beigezogen werden.

> Besteht eine gesetzliche oder vertragliche Geheimhaltungspflicht, so **dürfen die Daten nicht in einer Cloud bearbeitet werden** (Art. 11 Bst. b DSchG); das kann auch dazu führen, dass nur ein Teil der Datenbearbeitung ausgelagert werden darf.

> Für die Nutzung eines Cloud-Service zur Bearbeitung von Personendaten gelten die

Vorschriften für das «Bearbeiten im Auftrag» nach Artikel 18 DSchG. Das Bearbeiten von Personendaten darf nur dann an einen Cloud-Service-Anbieter übertragen werden, wenn das öffentliche Organ, das die Personendaten bearbeiten lässt, für den Datenschutz verantwortlich bleibt, dem Cloud-Service-Anbieter die erforderlichen Weisungen erteilt und dafür sorgt, dass er die Daten nur zur Erfüllung seines Auftrags verwendet oder bekanntgibt. Ist der Cloud-Service-Anbieter nicht dem DSchG unterstellt, wie dies bei Privatunternehmen der Fall ist, so stellt das öffentliche Organ den Datenschutz vertraglich sicher. So muss die Datensicherheit nach Artikel 22 DSchG und nach dem Reglement vom 29. Juni 1999 über die Sicherheit der Personendaten (DSR) garantiert sein. Nach diesen Bestimmungen **muss das öffentliche Organ, das Personendaten bearbeitet, die geeigneten organisatorischen und technischen Massnahmen treffen, um die Daten gegen jedes unerlaubte Bearbeiten zu schützen, und es muss für Vertraulichkeit, Verfügbarkeit und Integrität der Daten gesorgt sein**. Der Cloud-Service-Anbieter muss die Daten gegen folgende Risiken schützen: unbefugte oder zufällige Vernichtung oder zufälliger Verlust; technische Fehler; Fälschung; Diebstahl oder widerrechtliche Verwendung; unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen. Diese Massnahmen sind periodisch vor Ort zu überprüfen. Wie die Datenschutzanforderungen im Einzelnen umzusetzen sind, hängt vom Unternehmen bzw. der Behörde, von der Art der Daten, aber auch von der Organisation und vom Zuschnitt der Cloud-Lösung ab. Je nach Art des Cloud-Service, hier eine nicht abschliessende Aufzählung der Sicherheitsanforderungen: Sicherheitsmanagement; Virenschutz; Updates, Sicherheitsupdates; Backups und Wiederherstellung; Business Continuity; Authentifikation; Vertraulichkeit und Integrität der Datenflüsse; Kontrolle; Zurechenbarkeit und Rückverfolgbarkeit; Cloud-Service-Personal; Sicherheitsanforderungen an externes Personal. **Vertrauliche, geheime oder besonders schützenswerte Daten dürfen nicht in eine Cloud im Ausland ausgelagert werden.** Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte gibt die gleichen Empfehlungen an die öffentlichen Organe des Bundes ab. Es ist also auch möglich, dass nur ein Teil der Datenbearbeitung ausgelagert werden darf. Die Übermittlung von Personendaten der Webseitenbesucher ins Ausland unterliegt u.a. der Gefahr, dass ausländische Behörden aufgrund ihrer nationalen Gesetzgebungen auf die sich in ihrem Land befindlichen Daten zugreifen können.

> Der Dateninhaber muss sicherstellen, dass der Auftragsdatenbearbeiter die Daten nur so bearbeitet, wie er es selbst tun dürfte. Das öffentliche Organ muss also regelmässig abklären, ob die Datenbearbeitung ordnungsgemäss erfolgt, was einen grossen Kontrollaufwand bedeutet.

> Die Nutzung von Cloud Computing bedingt in vielen Fällen eine Datenbekanntgabe ins Ausland, da die Verarbeitung oftmals auf weltweit verstreuten Servern stattfindet. Sehr oft geht es dabei um Länder, die ein tieferes Datenschutzniveau als die Schweiz aufweisen. Personendaten dürfen **nur in Staaten bekannt gegeben werden, die einen angemessenen Schutz gewährleisten** (Art. 12a Abs. 1 DSchG). In Staaten, die keinen angemessenen Schutz gewährleisten, dürfen Personendaten jedoch bekannt gegeben werden, wenn eine der folgenden Bedingungen erfüllt ist: a) hinreichende Garantien, insbesondere vertragliche Garantien, gewährleisten einen angemessenen Schutz im Ausland; b) die betroffene Person hat im Einzelfall ausdrücklich eingewilligt; c) die Bearbeitung steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags und es handelt sich um Personendaten des Vertragspartners; d) die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung

von Rechtsansprüchen vor Gericht unerlässlich; e) die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen. Bei Übermittlung von Personendaten ins Ausland besteht auch die Gefahr, dass ausländische Behörden aufgrund ihrer nationalen Gesetzgebungen auf die sich in ihrem Land befindlichen Daten zugreifen können. Angesichts der Pflicht der öffentlichen Organe, die Personendaten der Bürger insbesondere vor unbefugten Zugriffen zu sichern, dürfte sich dieser Punkt als heikel erweisen. **Wichtig ist, dass grundsätzlich derjenige, welcher Personendaten ins Ausland übermittelt, nachweisen muss, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten.**

> Schliesslich ist der Cloud-Nutzer auch dafür verantwortlich, dass das Auskunftsrecht (Art. 23ff. DSchG) und das Recht auf Löschung und Berichtigung (Art. 26 DSchG) jederzeit gewährleistet sind und entsprechend den datenschutzrechtlichen Vorgaben umgesetzt werden. Dies kann mit erheblichen Schwierigkeiten verbunden sein, wenn der Cloud-Nutzer nicht weiss, wo die Daten bearbeitet werden.

Nach dem Gesagten stellen wir fest, dass eine gesetzliche Grundlage für die Auslagerung von Daten der öffentlichen Organe in eine Cloud fehlt. Somit ist das DSchG anwendbar. Die Auslagerung muss allerdings dem revidierten Bundesgesetz über den Datenschutz (DSG) und der daraus folgenden Revision des DSchG Rechnung tragen. Ausserdem müssen sich gemäss Gesetzgebung über das elektronische Patientendossier die Datenspeicher in der Schweiz befinden und dem Schweizer Recht unterstehen (Art. 25 Abs. 6 EPDV).

IV. Sonderfälle – Hosting in einer Cloud in der Schweiz oder in einer Cloud im Ausland

In diesem Fall bleiben das betroffene öffentliche Organ für seine Daten und das ITA für die IT-Sicherheit verantwortlich. Das ITA erteilt dem schweizerischen oder ausländischen Cloud-Service-Anbieter die erforderlichen Weisungen und sorgt auch dafür, dass sie eingehalten werden (Verordnung vom 3. November 2015 über das Informatik- und Telekommunikationsmanagement in der Kantonsverwaltung; SGF 122.96.11). So hängt die konkrete Umsetzung der organisatorischen und technischen Massnahmen davon ab, um was für Daten es sich handelt, wie die Cloud organisiert ist, wie gross die Risiken und wie vertraulich die Daten sind.

Insofern als praktisch in allen Dienststellen des Staates erst einmal die Mailanwendungen und dann die weiteren Applikationen ausgelagert werden sollen, sind wir der Ansicht, dass es eine staatliche freiburgische Cloud braucht. Damit liessen sich alle angesprochenen Risiken einschränken und die Kontrolle über alle vom Staat bearbeiteten Daten behalten.

Ohne freiburgische, westschweizerische oder nationale Cloud müssen restriktive technische und organisatorische Massnahmen getroffen werden, wenn der Staat sensible oder dem Amts-/Berufsgeheimnis unterliegende Daten bearbeitet.

Die sorgfältige Auswahl (inklusive Folgenabschätzung), Instruktion und Überwachung des Cloud-Service-Anbieters sind sehr wichtig bei einer Datenbearbeitung in der Cloud. Das öffentliche Organ bleibt gegenüber den betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und haftet bei allfälligen Verletzungen. Deshalb sollte es sich gut überlegen, welche Anwendungen und Daten es am eigenen Standort behalten will und welche in die Cloud ausgelagert werden sollen.

Dabei ist Folgendes zu beachten:

> die Private Cloud ist obligatorisch;

> die Daten dürfen nur in eine Cloud in der Schweiz oder in einem Staat mit einer Gesetzgebung, die ein hohes Datenschutzniveau bietet, ausgelagert werden;

> Daten, die dem Amts-/Berufsgeheimnis unterliegen, dürfen nicht ausgelagert, sondern müssen auf gesicherten staatlichen Servern gespeichert werden;

> sensible Daten müssen verschlüsselt übertragen und gespeichert werden; der Schlüssel muss beim öffentlichen Organ verbleiben, damit der Cloud-Service-Anbieter keinen Zugriff auf die Daten hat. Solche Daten dürfen ausserdem nur an Firmen ausgelagert werden, die ausschliesslich unter Schweizer Recht handeln, sich zur Mehrheit in Schweizer Eigentum befinden und ihre Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen;

> die Outsourcingbedingungen müssen in einem Vertrag festgelegt werden, der von der ÖDSB validiert werden muss. Das für die Daten verantwortliche öffentliche Organ muss den Outsourcingvertrag zudem genehmigen. Das ITA darf seinerseits keinen Standardvertrag unterzeichnen, der nicht personalisiert werden kann, sondern muss einen Vertrag für den gesamten Staat Freiburg mit besonderen Sicherheitsklauseln aushandeln. Vertraglich geregelt muss sein: Vertraulichkeit; unerlaubtes Erstellen von Profilen; Zweckbindung; keine Bekanntgabe an Dritte; Hosting und Speicherung; Übertragbarkeit; Aufbewahrungsdauer und Speicherung der Originaldaten; Auskunftsrecht; Kontrollen (insbesondere durch die ÖDSB); Datensicherheit: Virenschutz, Updates, Rückverfolgbarkeit, Datenvernichtung usw.;

> die Unterauftragsvergabe muss vom öffentlichen Organ genehmigt werden, das den entsprechenden Vertrag von der ÖDSB validieren lassen muss.

Wir weisen auch darauf hin, dass das Datenbearbeitungsangebot der Swisscom nicht DSchG-konform ist, da die Servicebeschreibung auf Leistungen von Microsoft verweist, gemäss den Geschäftsbedingungen von Microsoft, was nicht akzeptabel ist.

V. Fazit

Da eine gesetzliche Grundlage für die Auslagerung der Datenbearbeitung der öffentlichen Organe fehlt, gilt das DSchG.

Insofern als der Staat sensible und dem Amts-/Berufsgeheimnis unterliegende Daten bearbeitet, insbesondere in den Spitälern, Gefängnissen, bei der Kantonspolizei, den Gerichtsbehörden, der kantonalen Steuerverwaltung usw., soll eine staatliche freiburgische, westschweizerische oder nationale Cloud entwickelt werden, um die vollumfängliche Kontrolle über alle vom Staat bearbeiteten Daten zu behalten. So würden die Daten in den Händen des Staats bleiben.

Auch wenn das ITA vor allem finanzielle Gründe für die Auslagerung der Datenbearbeitung geltend macht, wird diese mit den Kontrollen der technischen und organisatorischen Massnahmen der ausgelagerten Daten zusätzlich zum Hosting von dem Amts- und/oder Berufsgeheimnis unterliegenden Daten beim Staat nicht rentabler, wohingegen eine staatliche Cloud den gesetzlichen Datenschutzanforderungen vollumfänglich und rechtsgenüglich entsprechen würde. Sie könnte ausserdem auch unseren Nachbarkantonen gegen Bezahlung zur Verfügung gestellt oder mit ihnen in Zusammenarbeit mit den anderen Kantonen entwickelt werden.

Ohne solche Cloud muss das ITA zwingend restriktive technische und organisatorische Massnahmen treffen, wobei Folgende zu beachten ist:

> die Private Cloud ist obligatorisch;

> die Daten dürfen nur in eine Cloud in der Schweiz oder in einem Staat mit einer Gesetzgebung, die ein hohes Datenschutzniveau bietet, ausgelagert werden;

> Daten, die dem Amts-/Berufsgeheimnis unterliegen, dürfen nicht ausgelagert, sondern müssen auf gesicherten staatlichen Servern gespeichert werden;

> sensible Daten müssen verschlüsselt übertragen und gespeichert werden; der Schlüssel muss beim öffentlichen Organ verbleiben, damit der Cloud-Service-Anbieter keinen Zugriff auf die Daten hat. Solche Daten dürfen ausserdem nur an Firmen ausgelagert werden, die ausschliesslich unter Schweizer Recht handeln, sich zur Mehrheit in Schweizer Eigentum befinden und ihre Leistung gesamtheitlich innerhalb der Schweizer Landesgrenzen erzeugen;

> die Outsourcing-Bedingungen müssen in einem Vertrag festgelegt werden, der von der ÖDSB validiert werden muss. Das für die Daten verantwortliche öffentliche Organ muss den Outsourcingvertrag zudem genehmigen. Das ITA darf seinerseits keinen Standardvertrag unterzeichnen, der nicht personalisiert werden kann, sondern muss einen Vertrag für den gesamten Staat Freiburg mit besonderen Sicherheitsklauseln aushandeln. Vertraglich geregelt muss sein: Vertraulichkeit; unerlaubtes Erstellen von Profilen; Zweckbindung; keine Bekanntgabe an Dritte; Hosting und Speicherung; Übertragbarkeit; Aufbewahrungsdauer und Speicherung der Originaldaten; Auskunftsrecht; Kontrollen (insbesondere durch die ÖDSB); Datensicherheit: Virenschutz, Updates, Rückverfolgbarkeit, Datenvernichtung usw.;

> die Unterauftragsvergabe muss vom öffentlichen Organ genehmigt werden, das den entsprechenden Vertrag von der ÖDSB validieren lassen muss.

Laurent Schneuwly
Präsident