Appenzell Ausserrhoden

Datenschutz-Kontrollorgan

Poststrasse 23
9001 St. Gallen

Stefan Gerschwiler
lic. iur., Rechtsanwalt
Tel. 071 228 29 30
stefan.gerschwiler@ar.ch

Datenschutz-Kontrollorgan, 9001 St. Gallen

An den Kantonsrat

St. Gallen, 28. Februar 2025

Bericht 2024 des Datenschutz-Kontrollorgans

Sehr geehrter Herr Kantonsratspräsident
Sehr geehrte Damen Kantonsrätinnen
Sehr geehrte Herren Kantonsräte

Gerne berichte ich (im Sinne von Art. 27 Abs. 1 Bst. h Datenschutzgesetz, bGS 146.1) über meine Tätigkeit als Datenschutz-Kontrollorgan im Jahr 2024.

A. Tätigkeitschwerpunkte

1. Beratung von öffentlichen Organen

Die Beratungsanfragen von öffentlichen Organen haben im Berichtsjahr weiter leicht zugenommen (Berichtsjahr: 67, Vorjahr: 65).

Wohl fast kein Bericht über das Jahr 2024 kommt, angesichts der in diesem Bereich einer breiten Öffentlichkeit bekannt und bewusst gewordenen technischen Fortschritte, um die "Künstliche Intelligenz" herum. Datenschutzrechtliche (und weitere) Aspekte konnte ich anlässlich einer Podiumsdiskussion beim Kaderseminar der Regierung erörtern. Meine Empfehlung ist, dieses spannende, vielversprechende Thema mit Interesse und Offenheit anzugehen und eigene Erfahrungen zu sammeln, damit die Chancen und Risiken klarer fassbar werden.

Appenzell Ausserrhoden

Für mich weiterhin deutlich stärker im Fokus standen indes auch 2024 die bereits im Vorjahr prägenden Themen Cybersicherheit und Cloud Computing. Sie betreffen fast sämtliche öffentlichen Organe in Appenzell Ausserrhoden.

Nach Beurteilung der AR Informatik AG (ARI) existieren heute für bestimme Anwendungsbereich keine Alternativen zur Microsoft 365 Cloud, die risikoarm einführbar und funktionell gleichwertig sind. Auf Grundlage dieser Einschätzung hat der Regierungsrat im Oktober 2024 die Einführung von Microsoft 365 Cloud-Diensten in Kanton und Gemeinden bewilligt. Er hat mich dazu angehört.

Der in meinem Bericht 2023 beschriebene massive, erfolgreiche Cyberangriff auf die Microsoft Cloud wurde im Berichtsjahr vom Cyber Safety Review Board des United States Department of Homeland Security untersucht. Das Board hält in seinem Untersuchungsbericht vom März 2024 fest, dass dieser Einbruch "vermeidbar war und niemals hätte geschehen dürfen." Das Board kam ferner zum Schluss, dass "die Sicherheitskultur von Microsoft unzureichend war und einer Überholung bedarf, insbesondere angesichts der zentralen Stellung des Unternehmens im Technologie-Ökosystem". Dabei verwies es auf "die Kaskade von vermeidbaren Microsoft-Fehlern, die diesen erfolgreichen Einbruch ermöglicht haben."

ARI wird bei der Einführung der Microsoft 365 Cloud-Dienste Verschlüsselungsmassnahmen umsetzen. Diese erhöhen in vielen Konstellationen den Schutz gegen unerlaubten Zugriff von Dritten auf die Daten. Microsoft muss aber den zur Verschlüsselung der in der Microsoft-Cloud liegenden Daten eingesetzten Schlüssel zu deren Entschlüsselung verwenden, um gewisse Dienste im Rahmen von Microsoft 365 überhaupt zur Verfügung stellen zu können, z.B. eine Suchfunktion für E-Mail-Inhalte. Microsoft wird mithin technisch in der Lage sein, die Daten im Klartext auszulesen. Damit verbleiben die prinzipiellen Restrisiken, dass diese Daten im Rahmen zukünftiger erfolgreicher Angriffe auf Microsoft auch von Dritten unbefugt ausgelesen werden können und dass US-amerikanische Regierungsstellen auch weiterhin in grossem Umfang die Herausgabe von Daten aus der Microsoft-Cloud anfordern (siehe auch hierzu meinen Bericht 2023).

Nach der publizierten Praxis der Konferenz der schweizerischen Datenschutzbeauftragten (privatim), kann bei der Bearbeitung besonders schützenswerter Personendaten durch Cloud-Dienstleister eine Verschlüsselung beim Cloud-Anbieter geprüft werden, wenn sich daraus keine untragbaren Risiken für die Grundrechte der betroffenen Personen ergeben. Der Cloud-Anbieter muss sich insbesondere vertraglich verpflichten, die Schlüssel nur mit der ausdrücklichen Zustimmung des öffentlichen Organs zu verwenden. Eine entsprechende klare Zusicherung mit Bezug auf Anforderungen von US-amerikanische Regierungsstellen auf Datenherausgabe gibt Microsoft aber nicht ab.

Auf (von mir ausdrücklich unterstützter) Empfehlung von ARI hat der Regierungsrat den Auftrag erteilt, einheitliche und verbindliche Weisungen für die Nutzung von Microsoft 365 Cloud-Diensten auszuarbeiten, welche insbesondere die Speicherung von als geheim klassifizierten Daten (Amts- und Steuergeheimnis, etc.) sowie von besonders schützenswerten Personendaten regelt. Die Arbeiten dazu haben im Berichtsjahr begonnen und werden 2025 abgeschlossen sein. Die Gemeinden werden dazu angehört.

Letztlich das grösste Risiko besteht beim Einsatz von Microsoft 365 Cloud-Diensten nach meiner Beurteilung darin, dass die bereits bestehende Abhängigkeit von Microsoft erheblich verschärft wird - und damit von einem ausländischen Anbieter, der seine in vielen Bereichen bereits heute erreichte Monopolstellung weiter ausbaut

Appenzell Ausserrhoden

und der bezüglich seiner bisherigen Anstrengungen im Bereich der Daten- und Cybersicherheit klar nicht überzeugt. Mittelfristig gefährdet diese Abhängigkeit als Klumpenrisiko Grundvoraussetzungen der staatlichen Aufgabenerfüllung in unserer digitalisierten Welt.

Die angesprochenen Risiken wurden auch auf nationaler Ebene erkannt. Im Dezember 2024 hat der Bundesrat die aktualisierte Strategie Digitale Schweiz für das Jahr 2025 verabschiedet und neue Fokusthemen festgelegt. Er will insbesondere die Informationssicherheit und Cybersicherheit für die gesamte Schweiz stärken und Open Source Software in der Bundesverwaltung fördern. Die Bundesversammlung hat im Berichtsjahr die gesetzlichen Grundlagen und einen Kredit in der Höhe von 246,9 Millionen Franken für die Schaffung einer Swiss Governement Cloud verabschiedet. Diese wird von Kantonen, Städten und Gemeinden genutzt werden können.

Auf (von mir ebenfalls ausdrücklich unterstützter) Empfehlung von ARI hat der Regierungsrat zusammen mit seiner Bewilligung der Einführung von Microsoft 365 Cloud-Diensten zugleich den Auftrag erteilt, eine Exit-Strategie zu erarbeiten. Als Elemente davon sehe ich etwa die Unterstützung entsprechender Bestrebungen auf nationaler Ebene, namentlich der Swiss Government Cloud, die Implementierung von Ausschreibungskriterien bei künftigen IT-Beschaffungen, die eine Unabhängigkeit von Microsoft positiv gewichten, und das Planen und Bereithalten kurzfristig einsetzbarer Ersatzlösungen, die öffentlichen Organen beim Ausfall der Microsoft 365 Cloud-Dienste wenigstens eine rudimentäre Grundfunktionalität (z.B. Kommunikationsfähigkeit) zur elementaren Aufgabenerfüllung bieten.

Die Wirksamkeit der in Appenzell Ausserrhoden bei der Nutzung von Microsoft 365 Cloud-Diensten zu treffenden Massnahmen (Nutzungsweisung, Exit-Strategie), hängt ganz wesentlich von deren Ausgestaltung, Implementierung und Durchsetzung ab. Hier erwartet uns viel Arbeit.

Relativ viele Beratungsanfragen kamen im Berichtsjahr wiederum aus dem Bereich des Departements Gesundheit und Soziales.

Die Komplexität beim Zusammenspiel der zahlreichen Akteure und Finanzierungsströme im Gesundheitswesen, z.B. bei der Pflegefinanzierung, zeigt sich auch in datenschutzrechtlichen Aspekten. So wurde ich gebeten zu beurteilen, inwieweit die (mitfinanzierenden) Gemeinden Einsicht in Rechnungen von Leistungserbringern der ambulanten Pflege nehmen dürfen. Hier stehen sich berechtigte, nachvollziehbare Informationsbedürfnisse der Gemeinden und ebenso berechtigte und nachvollziehbare Interessen der betroffenen Empfänger dieser Pflegeleistungen am Schutz der dabei zu bearbeitenden Angaben zu ihrer Gesundheit gegenüber. Die vertiefte Analyse der Rechtslage, bei der bundes- und kantonalrechtliche Sondernormen aus KVG (SR 832.10), PFG (bGS 833.15) und PFV (bGS 833.151) hineinspielen, hat gezeigt, dass hier noch Regelungslücken bestehen. Ich habe daher empfohlen, diesen Punkt bei nächster sich bietender Gelegenheit zur Anpassung der Verordnung über die Pflegefinanzierung zu präzisieren bzw. zu ergänzen.

Empfehlungen habe ich auch abgegeben zur Ausgestaltung der Datenbearbeitung bei der Evaluation von Amtsarzt- und Notfalldiensteinsätzen und zu den im Zusammenhang mit einem Masernfall im Umfeld einer Bildungseinrichtung gestützt auf das Epidemiengesetz (SR 818.101) zu treffenden Massnahmen der Kantonsärztin.

Appenzell Ausserrhoden

Die kantonale Steuerverwaltung habe ich im Berichtsjahr bei den Umsetzungsarbeiten zur im Vorjahr gefundenen Lösung für die Übermittlung von Daten aus dem Bereich des Steuerbezugs (Debitorenlisten) an die Gemeinden begleitet. Die detaillierten Informationen dazu finden sich auf dem über die Website der Steuerverwaltung abrufbaren Merkblatt.

Im Staatsarchiv konnte ich im Rahmen eines Workshops verschiedene datenschutzrechtliche Fragen erörtern. Beim Entscheid, inwieweit es eine Einsichtnahme in archivierte Personendaten ermöglich, muss das Staatsarchiv gestützt auf die einschlägigen Rechtsgrundlagen im Archivgesetz (bGS 421.10) und im Informationsgesetz (bGS 133.1) regelmässig eine Interessenabwägung vornehmen. Diese ist nicht immer einfach und das Staatsarchiv macht es sich auch nicht einfach, sondern handelt, soweit für mich beurteilbar, mit der gebotenen Umsicht.

Auf Einladung des Departements Inneres und Sicherheit habe ich mich zum Vorhaben der KKJPD vernehmen lassen, per Konkordat einen schweizweiten Polizeidatenraum zu schaffen. Die zunächst vorgeschlagene Regelung habe ich als unvollständig, unausgewogen und wenig durchdacht beurteilt; sie ritzte ohne Not die verfassungsmässige Kompetenzordnung, verfehlte die bei der Einschränkung von Grundrechten nach unserer Bundes- und Kantonsverfassung einzuhaltenden Hürden und verletzte datenschutzrechtliche Vorgaben aus Staatsvertrags-, Bundes- und kantonalem Recht. Im Oktober hat das Bundesgericht in seinem Urteil zum revidierten Polizeigesetz des Kantons Luzern festgehalten: "Sollte der Gesetzgeber tatsächlich einen voraussetzungs- und schrankenlosen Austausch sämtlicher polizeilicher Daten im Abrufverfahren zulassen wollen, verstiesse die Bestimmung gegen das Erfordernis eines überwiegenden öffentlichen Interesses und gegen das Verhältnismässigkeitsprinzip. Denn es ist nicht nachvollziehbar, inwiefern für sämtliche Polizeidaten, einschliesslich Bagatellfällen, ein Zugriff im Abrufverfahren erforderlich ist." Die KKJPD hat in der Folge beschlossen, die Frage des interkantonalen Polizeidatenaustauschs bzw. der künftigen Ausgestaltung der notwendigen Rechtsgrundlagen vertieft zu prüfen. Das Thema dürfte auch den Kantonsrat im Rahmen der laufenden Totalrevision des Polizeigesetzes beschäftigen.

Gemeinden habe ich im Berichtsjahr beispielsweise beraten zur Frage, wie beim Ausstellen einer Erbbescheinigung mit Angaben zu einer Person umzugehen ist, welche die Bekanntgabe ihrer Daten an Dritte durch die Einwohnerkontrolle sperren liess, oder wie sich ein Formular gestalten lässt, mit dem Lehrpersonen ihre Einwilligung zur Publikation von Fotos erteilen, die in verschiedenen Kontexten (z.B. Stellenantritt, Schulfasnacht) aufgenommen wurden und über verschiedene Medien (Website, Schulzeitung) verbreitet werden.

Die Gemeinde Lutzenberg hat beim nach Art. 24a Polizeigesetz (bGS 521.1) zuständigen Departement Inneres und Sicherheit ein Gesuch für eine Videoüberwachung mit Personenidentifikation auf öffentlichem Grund (Schulanlage Gitzbüchel) gestellt. Ich habe dieses zur Genehmigung empfohlen, aus den folgenden Überlegungen: Auf dem Schulareal Gitzbüchel lag nachgewiesenermassen eine auffällige Häufung von eher geringfügigen Sachbeschädigungen vor. Teilweise wurde Schaden durch Feuer angerichtet, woraus sich ein erhöhtes Risiko bzw. Schadenpotential ergibt. Das Interesse, eine konkrete Häufung von Straftaten an einem bestimmten Ort zu bekämpfen, indem zur Unterstützung der Tataufklärung und zur Abschreckung eine Videoüberwachungsanlage installiert wird, kann in die Abwägung einbezogen werden, die bei der damit verbundenen Einschränkung der Grundrechte der von der Überwachung betroffenen Personen vorzunehmen ist, und dieses Interesse kann die Einschränkung unter Umständen rechtfertigen. Ein Schulareal weist die Besonderheit auf, dass zahlreiche Personen, darunter insbesondere Kinder und Jugendliche, darauf angewiesen bzw. hoheitlich verpflichtet sind, sich dort aufzuhalten. Das stellt den Staat vor die Herausforderung, unnötige Eingriffe in die

Appenzell Ausserrhoden

Persönlichkeitsrechte dieser Personen zu unterlassen, sie insbesondere nicht ohne Not einem Überwachungsdruck auszusetzen und dabei zugleich ein sicheres Umfeld zu gewährleisten. Zur Entschärfung dieses Zielkonflikts ist die Videoüberwachung auf die schulfreie Zeit zu beschränken. Die Situation bezüglich Sachbeschädigungen kann sich durchaus ändern. Ich habe daher empfohlen, die Bewilligung jeweils für einen befristeten, verlängerbaren Zeitraum zu erteilen, wie das auch bei anderen bewilligten Videoüberwachungen der Fall ist.

2. Zusammenarbeit mit anderen Kantonen und Bund

Die Kooperation mit anderen Datenschutzaufsichtsstellen war im Berichtsjahr und bleibt auch in Zukunft für meine Tätigkeit wichtig. Die Vorteile einer engen Zusammenarbeit anerkennen auch die Regierungen der Kantone Appenzell Ausserrhoden, Appenzell Innerrhoden, St. Gallen und Thurgau. Sie liessen, unter Einbezug der kantonalen Datenschutzbeauftragten, die Möglichkeiten einer engeren Zusammenarbeit prüfen und haben dazu eine Vereinbarung ausgearbeitet mit dem Ziel der Stärkung der Qualität und der Effizienz des Datenschutzes in den vier Kantonen. Die Vereinbarung sieht die Schaffung einer im Kanton Thurgau anzusiedelnden Teilzeitstelle vor, die eine stärkere Nutzung der Synergien bei kantonsübergreifenden Aufgaben und Projekten ermöglichen soll.

Die Konferenz der schweizerischen Datenschutzbeauftragten privatim hat im Berichtsjahr ihre elektronische Austauschplattform in Betrieb genommen. Sie ist insbesondere bei der Koordination von Vernehmlassungen zu nationalen und kantonsübergreifenden Rechtsetzungsvorhaben hilfreich. Privatim bot auch den passenden Rahmen für die Beurteilung datenschutzrechtlicher Aspekte bei der Überarbeitung der sehr praxisrelevanten AGB für IKT-Leistungen, die von der Digitalen Verwaltung Schweiz zur Verfügung gestellt werden.

3. Beratung von Privaten

Auf relativ tiefem Niveau schwanken die Beratungsanfragen von Privatpersonen. Im Berichtsjahr war hier mit 11 Anfragen, nach dem vermutlich durch das Inkrafttreten des revidierten Datenschutzgesetzes des Bundes mitverursachten Höchststand im Vorjahr (23 Anfragen), ein Ausschlag nach unten zu verzeichnen, dabei allerdings mit Tendenz zu komplexeren Fragestellungen.

Beraten habe ich etwa zur Sperrmöglichkeit bei der Motorfahrzeughalterdatenauskunft, zum Einsichtsrecht bzw. Auskunftsanspruch bei logopädischen Behandlungen und beim Aufenthalt in einer Stätte für betreutes Wohnen sowie zum Anspruch auf Löschung von Daten bei der Polizei und der KESB.

Appenzell Ausserrhoden

B. Aufsichts- und Kontrolltätigkeit

Meine Aufsichts- und Kontrolltätigkeiten bewegten sich im Berichtsjahr (8) im vergleichbaren Umfang wie im Vorjahr (10).

Ein eigentlicher Klassiker einer Datensicherheitsverletzung hat sich im Berichtsjahr bei uns im Kanton ereignet, im Kontext der Bearbeitung von Daten zu Massnahmen im Bereich des Kindes- und Erwachsenenschutzes (aber nicht bei der KESB). Durch eine Fehlbedienung wurden beim Versand eines E-Mails den Empfängern auch alle weiteren Empfänger offengelegt, womit Rückschlüsse auf das Bestehen erwähnter Massnahmen bei diesen Personen möglich waren. Das betroffene öffentliche Organ hat in Absprache mit mir umgehend Massnahmen eingeleitet, um das Risiko weiterer ähnlicher Vorfälle zu senken.

Die Protokollierung der Zugriffe auf die Daten der kantonalen Einwohnerdatenplattform hat keine groben Auffälligkeiten gezeigt. Hier ist eine Tendenz zu verzeichnen, dass öffentliche Organe vermehrt Zugriff auf die AHV-Nummer wünschen. Dabei sind strenge bundesrechtliche Vorgaben zu beachten, deren vollständige Umsetzung im Kanton noch nicht abgeschlossen ist. Vorsicht ist beim Umgang mit diesem persönlichen, lebenslang unveränderlichen und eindeutigen Identifikator durchaus geboten. Das zeigt etwa die Warnung des Bundesamts für Cybersicherheit vom November 2024, es seien vermehrt Phishing-Mails im Namen von AHV-Ausgleichskassen zu beobachten, die den Empfängern eine angebliche Rückerstattung in Aussicht stellen und die Angabe von Kreditkarteninformationen verlangen. Es liegt auf der Hand, dass bei zunehmender Verbreitung der AHV-Nummer in online angreifbaren Systemen das Risiko ihrer missbräuchlichen Verwendung z.B. für derartige Phishing-Angriffe steigt.

Als sehr gut darf ich die Zusammenarbeit mit dem CISO der AR Informatik AG (vgl. Art. 18 Abs. 3 eGovG, bGS 142.3) bezeichnen. Wir tauschen uns regelmässig über Störungs- und Sicherheitsmeldungen aus und besprechen technische und organisatorische Massnahmen zur Stärkung der Datensicherheit. Dazu gehören auch die regelmässige Schulung und Sensibilisierung der ARI-Kundschaft. Trotz nach meiner Beurteilung erheblicher und zielgerichteter entsprechender Anstrengungen seitens ARI hat ein im Berichtsjahr durchgeführter Phishing-Test leider nicht durchwegs erfreuliche Resultate erbracht. Rund 6% der getesteten Mitarbeitenden haben sich dazu verleiten zu lassen, sich mit ihrem Usernamen und Passwort auf einer kantonsfremden Website zu registrieren, um einen angeblichen Rabatt auf ein Fitnessabo in Anspruch zu nehmen. Sie wurden von ARI zu Nachschulungen aufgeboten.

Gewisse Veränderungen sind bei meiner Aufsichts- und Kontrolltätigkeit mit der im Berichtsjahr abgeschlossenen, per 2025 in Kraft getretenen Teilrevision des kantonalen Datenschutzgesetzes absehbar. So werden öffentliche Organe neu im Rahmen von Datenschutz-Folgenabschätzungen vor jeder systematischen Bearbeitung von Personendaten das Risiko für eine damit verbundene Beeinträchtigung von Grundrechten der betroffenen Personen zu prüfen und es soweit möglich und zumutbar durch technische und organisatorische Massnahmen zu beschränken haben. Ist das Risiko hoch, muss bei mir eine Vorabkonsultation erfolgen. Neu ist auch die Pflicht zur Meldung von Verletzungen der Datensicherheit an mich. Die praktischen Auswirkungen dieser Änderungen bleiben abzuwarten. Ich sehe jedenfalls nicht vor, mein Rollenverständnis als in erster Linie auf Kooperation setzende, beratende und vermittelnde Instanz aufzugeben.

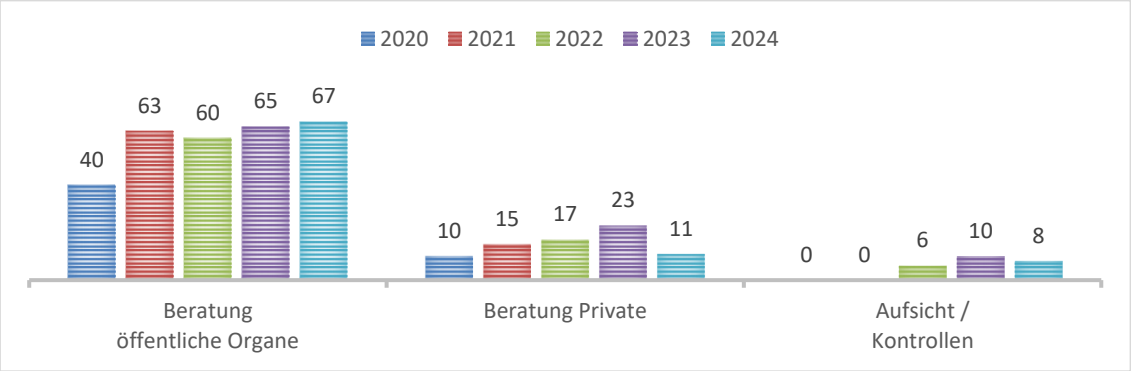
Als gleichsam erster Vorbote kommender Herausforderungen hat im Berichtsjahr eine grosse Privatklinik-Gruppe, die schweizweit und auch in Appenzell Ausserrhoden tätig ist, eine Datenschutzfolgeabschätzung im

Appenzell Ausserrhoden

Zusammenhang mit der Bearbeitung von Gesundheitsdaten unter Einsatz eine Cloud-Lösung zur (durch privatim koordinierten) Vorabkonsultation unterbreitet.

C. Ressourcen / Entwicklung

Die Entwicklung der Fallzahlen in den einzelnen Aufgabenbereichen zeigt sich grafisch folgendermassen:



D. Schlussbemerkungen und Antrag

"Gesetze sind wie Würste; man sollte besser nicht dabei sein, wenn sie gemacht werden." Nach den positiven Erfahrungen mit der im Berichtsjahr abgeschlossenen Teilrevision des kantonalen Datenschutzgesetzes kann ich dieses Bonmot nicht teilen. Gemäss der auf Seite 2 dieses Berichts dargestellten Situation scheint es mir viel besser auf die Produkte gewisser Cloud-Anbieter zuzutreffen; die gab es bei der Prägung der Redewendung allerdings noch nicht.

Appenzell Ausserrhoden

Ich ersuche Sie, sehr geehrter Herr Kantonsratspräsident, sehr geehrte Damen Kantonsrätinnen und Herren Kantonsräte, vom vorliegenden Bericht wohlwollend Kenntnis zu nehmen,

und entbiete an dieser Stelle Ihrer GPK, Ihrer KIS, der Kantonskanzlei, dem Departement Inneres und Sicherheit, dem Departement Finanzen und der AR Informatik AG meinen besonderen Dank für die gute Zusammenarbeit bei der Gewährleistung des Datenschutzes in Appenzell Ausserrhoden im Berichtsjahr.

Datenschutz-Kontrollorgan

Stefan Gerschwiler