**Konova AG**
Feldhof 2, 6300 Zug
041 511 80 20
info@konova.ch
konova.ch

# Interview mit Rechtsanwalt Lukas Fässler, FSDZ Rechtsanwälte & Notariat AG, 6340 Baar

Geführt von Miro Hegnauer, Inhaber und Geschäftsführer Konova AG

**Miro Hegnauer:** Vielen Dank Herr Fässler, dass Sie sich zu diesem Interview betreffend Datenschutz und Datensicherheit von E-Partizipationslösungen bereiterklärt haben. Erzählen Sie uns etwas über sich, was sind Ihre Schwerpunktgebiete?
**Lukas Fässler:** Ich bin der Senior Rechtsanwalt der Kanzlei FSDZ Rechtsanwälte & Notariat AG, einer Wirtschaftsanwaltskanzlei mit Schwerpunkt Informatik- und Kommunikationsrecht, Datenschutz- und Sicherheitsrecht, Werbe- und Wettbewerbsrecht sowie Cyberkriminalität. Ebenfalls sind wir spezialisiert für öffentliches Beschaffungsrecht im ITC-Umfeld öffentlich-rechtlicher Körperschaften wie Städte, Gemeinde und Kantone. Ich bin seit 1997, also seit über 23 Jahren, Spezialanwalt mit diesen Schwerpunkten. Davor war ich von 1992-1997 Informatikchef des Kanton Luzern.

**Miro Hegnauer:** Wie wichtig ist der Datenschutz und die Datensicherheit für eine E-Partizipationslösung?
**Lukas Fässler:** Grundsätzlich sehr wichtig. Datenschutz und Datensicherheit schaffen Vertrauen bei jenen Personen, die in einem digitalen Partizipationsprozess mitwirken möchten. Jeder Teilnehmer gibt je nach Umfrage wertvolle und zum Teil sehr persönliche Ansichten und Informationen bekannt, die mit grosser Wahrscheinlichkeit dem Datenschutz unterliegen und deshalb die öffentlich-rechtlichen Körperschaften zu einem gesetzeskonformen Umgang mit diesen Bürgerdaten verpflichten. Wichtig dabei ist, dass diese Umfragedaten über organisatorische und technische (Sicherheits-)Massnahmen so geschützt werden, dass eine missbräuchliche Verwendung ausgeschlossen oder mit hoher Wahrscheinlichkeit unterbunden werden kann. Dafür ist die Behörde verantwortlich, welche über eine E-Partizipationslösung Umfragedaten ihrer Einwohner erhebt und dann auswertet. Es ist daher auch immer die Aufgabe einer solche Behörde zu prüfen, ob sie für die Durchführung solcher Umfragen über eine genügende gesetzliche Grundlage verfügt oder das ausdrückliche Einverständnis der Befragten zur Bearbeitung ihrer Daten eingeholt wurde und nachgewiesen werden kann.

**Miro Hegnauer**: Auf was sollte bei der Beschaffung einer solchen E-Partizipationslösung Wert gelegt werden?
**Lukas Fässler**: Es gibt natürlich viele Punkte, die zu beachten sind. Grundsätzlich ist es aber wichtig für die Behörde festzustellen, dass der Anbieter sich umfassende Gedanken zum Thema Datenschutz- und Datensicherheit gemacht und entsprechende Massnahmen umgesetzt hat. Die Behörde sollte sich die entsprechenden Konzeptgrundlagen zum Datenschutz und zur Datensicherheit des Anbieters zeigen lassen. Sehr gute Software-Anbieter sind in der Lage, der öffentlich-rechtlichen Körperschaft ein schriftlicher Datenschutz- und Sicherheitskonzept über die einzusetzende E-Partizipationslösung nach den Grundsätzen «privacy by default» und «privacy by design» vorzulegen.
Dazu kommen weitere Grundsatzüberlegungen wie beispielsweise die Hoheit über die gesammelten Personen- und Sachdaten. Die Hoheit und damit die Verantwortung über solche Daten muss beim Verantwortlichen, also bei der Gemeinde, bei der Stadt oder beim Kanton liegen und nicht beim Anbieter der E-Partizipationslösung (Lizenzgeberin oder Betriebs-Dienstleisterin). Das heisst, der Kunde der E-Partizipationslösung (die Behörde) ist im Sinne des Datenschutzrechts als Verantwortlicher zu Einhaltung der Datenschutz- und Datensicherheitsvorgaben verpflichtet.
Ein weiterer wichtiger Punkt ist die Datenintegrität. Eine E-Partizipationslösung muss die Richtigkeit, die Vollständigkeit und die Konsistenz von erhobenen Daten gewährleisten können, damit die Auswertung der Daten auch verlässliche und richtige Resultate liefert.

**Miro Hegnauer**: Wie sieht es aus mit der Übertragung und der Verarbeitung von Daten? Welche Punkte müssen hier beachtet werden?
**Lukas Fässler**: Wird die Bearbeitung der gesammelten Umfragedaten ganz oder teilweise durch Partner der E-Partizipationslösung unterstützt (z.B. Rechenzentrumsdienstleisterin), muss die Behörde mit diesem Verarbeiter eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung (ADVV) abschliessen. Denn die Behörde muss nach den Regeln des Datenschutzrechtes nachweisen können, dass sie die ihr selber auferlegten Verpflichtungen zur Einhaltung des Datenschutzes im notwendigen Umfang an den beigezogenen Datenverarbeiter vollumfänglich übertragen hat. Gibt die Behörde dem beigezogenen Datenverarbeiter für die Bearbeitung von Personendaten keine Vorgaben, verletzt sie die Bestimmungen des Datenschutzgesetzes und hat dafür die Verantwortung zu übernehmen.
Es ist auch dringend zu empfehlen, die Speicherung und die Verarbeitung der erhobenen Personendaten wenn immer möglich in einem zertifizierten (z.B. ISO27001) Rechenzentren mit Sitz in der Schweiz vorzunehmen. So kann sichergestellt werden, dass der beigezogene Service-Dienstleister unter dem gleichen Datenschutzrecht steht wie die Behörde selber und auch wie der Anbieter der E-Partizipationslösungen selbst. Die Rechtsansprüche gegen die Vertragspartner lassen sich zuverlässig nur unter diesen Vorgaben durch eine Behörde durchsetzen.

**Miro Hegnauer:** Was müssen Anbieter von E-Partizipationslösungen beachten?
**Lukas Fässler:** Natürlich müssen sie sämtliche Anforderungen des Schweizer Datenschutzgesetz (DSG) erfüllen. Dazu ist gerade jetzt zu beachten, dass wir kurz vor der Einführung eines neuen Datenschutzrechtes in der Schweiz stehen, das sich grossmehrheitlich auf die Europäischen Vorgaben der Datenschutz-Grundverordnung (DSGVO) abstützt.

Anbieter von E-Partizipationslösungen müssen insbesondere als Lizenzgeber die Grundsätze von «privacy by default» und «privacy by design» bei der Entwicklung ihrer Lösungen berücksichtigten. Dazu gehört etwa ein angemessenes Benutzerberechtigungssystem mit Rollen und entsprechend eingeschränkten oder erweiterten Datenbearbeitungsrechten je nach Aufgabenbereich der betroffenen Personen. Zweitens ist darauf zu achten, dass insbesondere bei der Erhebung von Personendaten sparsam mit solchen Erhebungen umgegangen wird und wirklich nur jene Informationen abgefragt werden, die für die entsprechende Umfrage notwendig sind. Solche Daten sind dann nach deren Auswertung allenfalls wieder zu vernichtet. Das Anlegen von Datenfriedhöfen ist unter dem Datenschutzgesetz nicht erlaubt.

**Miro Hegnauer:** Immer mehr Services können aus der Cloud bezogen werden, so auch Partizipationslösungen. Ist der Einsatz einer SaaS-Lösungen für Verwaltungen aus datenschutzrechtlicher Perspektive überhaupt praktikabel?
**Lukas Fässler:** Ja, sofern die entsprechenden Rahmenbedingungen eingehalten werden. Viele Verwaltungen sind bezüglich der Nutzung von Cloud-Lösungen noch skeptisch eingestellt. Wird jedoch ein Cloud-Service unter strikten Sicherheits- und Datenschutzanforderungen angeboten, wie dies z.B. bei der SaaS-Lösung «E-Mitwirkung» der Fall ist, sind diese Bedenken häufig unberechtigt. Vorteile wie eine schnelle Verfügbarkeit und ein geringer Wartungsaufwand sind weitere Argumente für den Bezug des Services aus der Cloud. Die Behörden haben gerade aber bei solchen Lösungen über ADVV sicherzustellen, dass der Cloud-Serviceanbieter in die Verpflichtungen des Datenschutzes eingebunden und über Service-Level-Agreements die technischen und organisatorischen Massnahmen (SLA TOM genannt) garantiert. Diese sind denn auch von den Behörden periodisch zu überprüfen.

**Miro Hegnauer:** E-Mitwirkung ist eine Schweizer Gesamtlösung für die digitale Mitwirkung. Sie beraten die Entwickler von E-Mitwirkung in datenschutzrechtlichen Themen. Ist die E-Partizipationslösung betreffend Datenschutz und Datensicherheit gut aufgestellt?
**Lukas Fässler:** Die Konova AG hat mich von Anfang an in die Lösungsentwicklung miteinbezogen. Datenschutz- und Sicherheitsüberlegungen konnten so von Beginn an in die Entwicklung und in die organisatorischen Prozesse integriert werden. Mit einem unabhängigen, strengen Review zum Thema Datenschutz- und Sicherheit konnten zusätzliche Empfehlungen erarbeitet werden, die durch die Konova AG implementiert wurden. Die Lösung wurde so bereits zu Beginn an viele der Normen der europäischen Datenschutzgrundverordnung (DSGVO) angepasst, welche deutlich weitergeht als das aktuelle DSG der Schweiz. Dies macht aber auch Sinn, denn das Schweizer DSG ist seit einiger Zeit in Anpassung und wird sich stark an der DSGVO orientieren. Die E-Mitwirkung entspricht somit hohen Datenschutz- und Sicherheitsstandards und erfüllt so die Erwartungen der Verwaltungen und den gesetzlichen Anforderungen. Verwaltungsbehörden sollen sich auch das Datenschutz- und Sicherheitskonzept der Konova AG zu ihrer E-Partizipationslösung zeigen lassen, um darauf basierend die benötigten ADVV und SLA TOM mit dem Cloud-Serviceanbieter und Cloud-Betreiber schriftlich festzulegen. Die Behörden sollen daran denken, dass sie periodische Ueberprüfungen der einmal vereinbarten Massnahmen vorsehen und dokumentiere.

**Miro Hegnauer:** Vielen Dank, dass Sie sich Zeit genommen haben für dieses Interview.
**Lukas Fässler:** Sehr gerne.

Zur Person:

Rechtsanwalt Lukas Fässler gilt als einer der bekanntesten und renommiertesten Informatik-Experten der Schweiz mit über 23-jähriger Praxiserfahrung. Seit 1982 befasst er sich hauptberuflich mit Informatik und Telekommunikation, Governance und Compliance von Unternehmen, insbesondere auch in Bezug auf Datenschutz- und Datensicherheitsanforderungen. Von 1992 bis 1997 leitete er als Informatikchef des Kantons Luzern die Organisations- und Informatik- Dienste (OID) des Kantons LU. Seit 1997 ist er Inhaber und Senior Legal Consultant bei FSDZ Rechtsanwälte & Notariat AG, deren Verwaltungsratspräsident er ist. Als Dozent an Fachhochschulen und an der Universität Basel sowie Bern/Lausanne vermittelt er praxiserprobtes IT-Rechtswissen. Als Verwaltungsrat nimmt er strategische Führungsverantwortungen bei verschiedenen privaten und öffentlich-rechtlichen IT-Service-Unternehmen wahr (https://www.fsdz.ch/team/faessler-lukas).