# Publis Public Info Services AG
# von Gemeinden für Gemeinden

## 40. Publis ePool-Event

## Datenschutz-Folgenabschätzung und IKT-Minimalstandards

Teams-Meeting, 20. März 2025; Fabio Kleiner, Aline Lorgé und Gérald Strub

# Agenda

1. Begrüssung und Vorstellung
2. Datenschutz-Folgenabschätzung
3. IKT-Minimalstandards
4. Diskussion und Fragen

# TRANSFORMATION DER ÖFFENTLICHEN VERWALTUNG

Die Publis Public Info Service AG berät, unterstützt und begleitet Aargauer Gemeinden und Schulen in allen Digitalisierungs-, Organisations-, Prozess- und Informatikfragen.

Zudem unterstützt die Publis Public Info Service AG ihre Kunden im öffentlichen Sektor bei personellen Vakanzen und bei der rechtlich korrekten Durchführung von Beschaffungsprozessen.

# Publis Leistungen

- **Organisation und Entwicklung**
  - Verwaltungsanalyse
  - Internes Kontrollsystem
  - ICT-Strategie und Konzepte
  - Strategie-Klausuren
- **Digitalisierung**
  - Kommunale Service-Erstellung
  - Prozessoptimierung in bestehender IT-Umgebung
  - Digital Manager auf Zeit
- **Beschaffung**
  - Beschaffungen nach IVöB
  - Vertragsmanagement
- **Interims-Management**

- Als Publis Aktionäre profitieren die Gemeinden von einem tieferen Stundenansatz und einer Dividende

# Agenda

1. Begrüssung und Vorstellung
2. **Datenschutz-Folgenabschätzung**
3. IKT-Minimalstandards
4. Diskussion und Fragen

# Datenschutz-Folgenabschätzung

» Wann und warum ist eine Datenschutz-Folgeabschätzung notwendig?

# Rechtliche Grundlagen

- § 17a Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG)
- § 6 Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG)

# Was ist eine Datenschutz-Folgenabschätzung?

» Eine systematische Analyse zur Bewertung der Auswirkungen einer Datenverarbeitung

» Notwendig bei voraussichtlich erhöhtem Risiko für die Persönlichkeit und die Grundrechte der betreffenden Person

# Indizien für ein erhöhtes Risiko (1/2)

- Das System-Profiling ermöglicht, dass Daten ausgewertet werden können, um wesentliche **persönliche Merkmale zu analysieren** oder **Entwicklungen hervorzusagen**, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität
- Die Bearbeitung besonders **schützenswerter Personendaten**
- Die **Bearbeitung von Personendaten wird nicht vom öffentlichen Organ selbst durchgeführt**, sondern durch einen Auftragnehmer, insbesondere wenn Cloud Services von Cloud-Anbietern zum Einsatz kommen
- **Zwei oder mehrere öffentliche Organe** bearbeiten Personendaten in einem gemeinsamen elektronischen System

# Indizien für ein erhöhtes Risiko (2/2)

- Eine **systematische Überwachung**
- Eine **umfangreiche Datenbearbeitung** (wenn bspw. mehr als 1000 Personen betroffen oder viele Arten von Daten gesammelt werden)
- Die Personendaten werden mit anderen Datenbeständen **abgeglichen** oder **verknüpft**
- Die Personendaten werden in **Länder ohne gleichwertige Datenschutzniveaus** übermittelt
- Verwendung **webbasierter Techniken**
- Verwendung **neuer Technologien** (z.B.: Gesichtserkennung)
- Verwendung optisch-elektronische Überwachungsanlagen (**Videoüberwachung**)

# Indizien für ein erhöhtes Risiko – Fazit

» **Faustregel**: Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn mindestens zwei der vorgenannten Indizien zutreffen.

» Auf die Datenschutz-Folgenabschätzung kann verzichtet werden, sofern und soweit die Datenbearbeitung in der gesetzlichen Grundlage ausdrücklich geregelt werden.

# Wann ist eine Datenschutz-Folgenabschätzung notwendig?

- Einführung neuer IT-Anwendungen zur Verarbeitung von Personendaten
  - Bsp. Einführung einer GEVER Lösung
- Wesentliche Erweiterung oder Änderung bestehender IT-Anwendungen
  - Bsp. Ersatz einer Gemeindefachlösung
- Die geplante Bearbeitung von Personendaten führt voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person
  - Bsp. Einführung einer Video-Überwachungsanlage

# Mindestinhalt Datenschutz-Folgenabschätzung

Gemäss § 6a VIDAG

- Das verantwortliche öffentliche Organ, die rechtliche Grundlage, den Zweck und eine systematische Beschreibung der geplanten Datenbearbeitung;
- Eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Datenbearbeitung in Bezug auf den Zweck:
- Eine Bewertung der Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen unter Beachtung der Schutzziele;
- Die technischen und organisatorischen Massnahmen, die zur Bewältigung der Risiken geplant sind, unter anderem in Bezug auf Datenbearbeitung durch beauftragte Dritte.

# Abschluss der Datenschutz-Folgenabschätzung

- Die Ergebnisse der Datenschutz-Folgenabschätzung sind schriftlich festzuhalten und aufzubewahren (Nachweisführung).
- Ergibt die Datenschutz-Folgenabschätzung ein effektiv erhöhtes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person ist die Öffentlichkeits- und Datenschutzbeauftragte über das Ergebnis der Datenschutz-Folgenabschätzung in Kenntnis zu setzen (zwecks Vorab-Konsultation).
- Im Sinne eines guten Datenschutz-Managements sollten Datenschutz-Folgeabschätzungen bestehender Informatikanwendungen laufend durchgeführt werden, spätestens jedoch alle drei Jahren.

# Wir unterstützen Sie gerne!

» **Individuelle Beratung:**
Wir helfen Ihnen zu prüfen, ob eine DSFA erforderlich ist.

» **Praxisnahe Umsetzung:**
Wir begleiten Sie durch den gesamten Prozess – von der Risikoanalyse bis zur Dokumentation.

» **Rechtssicherheit:**
Unsere Expertise sorgt dafür, dass Sie alle gesetzlichen Anforderungen erfüllen.

# Fazit

» Die Datenschutz-Folgenabschätzung ist ein zentrales Instrument zur Minimierung von Datenschutzrisiken.

» Eine frühzeitige und regelmässige Prüfung hilft, rechtliche und organisatorische Probleme zu erkennen und zu beheben.

# Agenda

1. Begrüssung und Vorstellung
2. Datenschutz-Folgenabschätzung
3. **IKT-Minimalstandards**
4. Diskussion und Fragen

# Einführungsvideo

# Was ist unter IKT-Minimalstandard zu verstehen?

- Standard für die Stärkung der Informations- und Kommunikationstechnologien (IKT)
  - In erster Linie an die Betreiber gerichtet, soll aber auch auf alle anderen Organisationen anwendbar sein (bspw. Gemeinden)
- IKT-Minimalstandards wurden durch die Wirtschaftliche Landesversorgung (Bund) erarbeitet und sind teilweise, bspw.in der Energiebranche zwingend umzusetzen
- Der Standard bietet Massnahmen zur konkreten Umsetzung der ausführenden Stelle
  - Für den Bereich «Öffentliche Verwaltung» gibt es aktuell noch keinen Minimalstandard, ist jedoch in Planung

# Rechtliche Grundlagen Kanton AG

- Gesetz über die Informationssicherheit im (InfoSiG)
  - Geplantes Inkrafttreten am 1. Juli 2026
  - Anhörung bereits erfolgt
- Aufgaben der Informationssicherheit werde heute im Rahmen der zur Verfügung stehenden Ressourcen wahrgenommen
  - Vorgaben sind jeweils eher verwaltungsintern nach Best Practices und nicht auf gesetzlichen Grundlagen

# Relevant für die Gemeinden…

*§ 1 Zweck*

*1 Dieses Gesetz bezweckt die Gewährleistung der sicheren Bearbeitung von Informationen sowie des sicheren Einsatzes der Informatikmittel durch die Behörden des Kantons.*

*2 Damit sollen die nachfolgenden öffentlichen Interessen geschätzt werden:*

*a) die innere Sicherheit,*

*b) die Entscheidungs- und Handlungsfähigkeit der Behörden und ihrer Verwaltungseinheiten sowie*

*c) Die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen des Kantons zum Schutz von Informationen.*

# Relevant für die Gemeinden…

*§ 2 Geltungsbereich*

*1 Dieses Gesetz gilt für den Grossen Rat, den Regierungsrat und die Gerichte (Behörden) sowie deren Verwaltungseinheiten.*

*2 Für die Gemeinden und andere Träger öffentlicher Aufgaben gelten die Bestimmungen über*

*a) die klassifizierten Informationen des Kantons, soweit sie klassifizierte Informationen des Kantons bearbeiten sowie*

*b) die Sicherheit beim Einsatz von Informatikmitteln, soweit auf Informatikmittel des Kantons zugegriffen wird.*

*3 Absatz 2 findet keine Anwendung, wenn die Gemeinden und andere Träger öffentlicher Aufgaben eine mindestens gleichwertige Informationssicherheit gewährleisten.*

# Relevant für die Gemeinden…

- Gemeinden sind mit zahlreichen kantonalen Systemen verbunden, bspw. im Bereich Steuern
  - Gesetzlichen Bestimmungen müssen zumindest im Zusammenhang mit den kantonalen Systemen künftig sichergestellt werden
  - Damit wird sichergestellt, dass sie zum Einfallstor für Angriffe auf kantonale Systeme werden.
- Regierungsrat sieht vor, dass die IKT-Minimalstandards des Bundes bis Ende 2026 erreicht werden sollen

# Fazit

- Mit der kantonalen Rechtssetzung müssen Gemeinden künftige Standards in diesem Bereich einhalten
- Der Bedarf an solchen Standards besteht jedoch völlig unabhängig davon
  - Gemeinden arbeiten mit eigenen IT-Infrastrukturen, oftmals im Betrieb durch externe Anbieter
  - Gestützt auf die internationalen Standards den Schutz von Informationen und Informatikmitteln zu gewährleisten und zur Risikominimierung beizutragen ist für die Gemeinden auch heute bereits unabdingbar

# Und nun – was heisst das für uns als Gemeinde?

- Wie erwähnt, gibt es für die Öffentliche Verwaltung keinen durch den Bund definierten Branchenstandard
  - Der IKT-Minimalstandard beschreibt einen SOLL-Zustand
  - Wie funktioniert die konkrete Umsetzung?
- Der Bund stellt ein Assessment-Tool zur Verbesserung der IKT-Resilienz zur Verfügung, welches aus unserer Sicht bei folgenden Ausgangslagen eingesetzt werden kann
  - Durchführung IKT-Minimalstandard-Assessment
  - ICT-Strategien und ICT-Konzepte
  - Öffentliche Beschaffung neuer Lösungen
- Zusätzlicher Leitfaden zur Umsetzung des Minimalstandards, welcher generisch für alle Branchen angewendet werden kann
  - Beantwortung der Frage, wie gelange ich vom IST- in den SOLL-Zustand

# Vorgehen

» Ausarbeitung des aktuellen Erfüllungsgrades sowie der daraus folgenden «Erfüllung des IKT-Minimalstandards»

» Aufgeteilt in fünf unterschiedliche Kapitel

# Identifizieren (Identify)

- Unter anderem beinhaltet dies…
  - Inventar Management; Was ist überhaupt alles vorhanden (Infrastruktur, Personen, Daten, usw.)
  - Governance; Wer leitet und überwacht die Cybersicherheit?
  - Risikoanalyse; Wie wirken sich die Risiken auf unseren Geschäftsalltag aus?

# Schützen (Protect)

- Unter anderem beinhaltet dies…
  - Zugriffsmanagement und –steuerung; Wer und welche Geräte haben Zugriff auf unsere Infrastruktur?
  - Sensibilisierung und Ausbildung; Wie stellen wir sicher, dass Mitarbeitende und externe Personen die nötigen Kenntnisse im Cybersicherheits-Bereich mitbringen?
  - Einsatz von Schutztechnologie; Haben wir technische Security-Lösung in Betrieb? Wer ist dafür zuständig?
  - Informationsschutzrichtlinien; Haben wir oder braucht es neue interne Weisungen zum Umgang mit der IKT?
  - Unterhalt; Durch wen und wie oft werden die Systeme gewartet?

# Erkennen (Detect)

- Unter anderem beinhaltet dies…
  - Auffälligkeiten und Vorfälle; Werden relevante Ereignisse (bspw. Angriffsversuche) erkannt?
  - Überwachung; Werden die Systeme überwacht? Wenn ja, wie oft und durch wen?
  - Detektionsprozesse; Prozesse und Handlungsanweisungen zur Detektion werden getestet und unterhalten (bspw. Testangriffe)

# Reagieren (Respond)

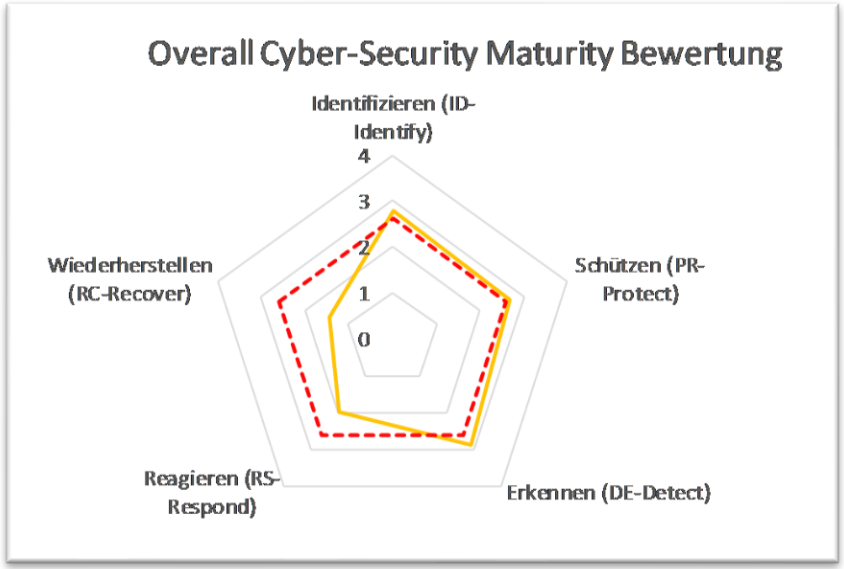
- Unter anderem beinhaltet dies…
  - Reaktionsplanung; Sind Reaktionsprozesse und –verfahren definiert und wie sehen diese aus?
  - Kommunikation; Wie werden die Reaktionsmassnahmen intern und extern kommuniziert und koordiniert?
  - Verbesserungen; Werden bestehende Reaktionsprozesse optimiert und aus vergangenen Vorfällen gelernt?

# Wiederherstellen (Recover)

- Unter anderem beinhaltet dies…
  - Wiederherstellungsplanung; Gibt es Wiederherstellungsprozesse und –verfahren? Wer ist dafür zuständig?
  - Verbesserungen; Wiederherstellungsplanung werden stets optimiert
  - Kommunikation; Die Wiederherstellungsaktivitäten werden mit internen und externen Stellen / Parteien koordiniert

# Ergebnis im Rahmen des Assessment-Tools

- Bewertungsschema der Aufgaben:
  - 0 = Nicht erfüllt
  - 1 = Partiell umgesetzt, nicht vollständig definiert und abgenommen
  - 2 = Partiell umgesetzt, vollständig definier und abgenommen
  - 3 = Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch
  - 4 = Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert
- Nach der Bewertung der 108 Aktivitäten ergibt sich ein „Overall Cyber Security Maturity Rating“
  - Standard gilt als erfüllt, wenn die Minimalvorgaben (rot) eingehalten werden



# Dienstleistungen der Publis

- Gerne unterstützen wir Sie bei den erwähnten Geschäftsfällen:
  - **Durchführung IKT-Minimalstandard-Assessment** – wie sind wir als Gemeinde heute aufgestellt?
  - **ICT-Strategien und ICT-Konzepte** – wie wollen wir in Zukunft aufgestellt sein mit unserem aktuellen externen Partner?
  - **Öffentliche Beschaffung** – wie wollen wir künftig mit einem neuen externen Partner aufgestellt sein?
- Wir begleiten Sie auch in der Umsetzung des Standards gemäss Leitfaden des Bundes, sodass von SOLL auch IST wird ☺

# Agenda

1. Begrüssung und Vorstellung
2. Datenschutz-Folgenabschätzung
3. IKT-Minimalstandards
4. **Diskussion und Fragen**

# Nächste Termine

» Publis Generalversammlung: 04. Juni 2025 um 10.30 Uhr in hybrider Form in Lenzburg.

» ePool Event 2: Donnerstag, 12. Juni 2025, 16.30 Uhr

» ePool Event 3: Donnerstag, 11. September 2025, 11.00 Uhr

» ePool Event 4: Donnerstag, 20. November 2025, 16.30 Uhr

# Abschluss

## Herzlichen Dank für Ihr Interesse und die Aufmerksamkeit!

- Bei Fragen wenden Sie sich gerne an
  - Fabio Kleiner, fabio.kleiner@publis.ch, 076 454 04 17
  - Aline Lorgé, aline.lorge@publis.ch, 076 582 17 96
  - Gérald Strub, gerald.strub@publis.ch, 079 622 73 55