Daten und Informationen sind das Gold des 21. Jahrhunderts

# Wann ist sicher wirklich sicher?

Nach einem Jahr Aufbauarbeit betreibt die Psychiatrische Dienste Aargau AG (PDAG) ein interdisziplinäres Datenschutz- und Informationssicherheits-Managementsystem. Die ersten Erfahrungen zeigen: Das System funktioniert und baut Mauern zwischen Organisationseinheiten ab.

Die PDAG handeln definitiv nicht mit Gold. Aber, die personenbezogenen Daten ihrer Patienten, Mitarbeitenden und Partner sind mindestens so wertvoll und daher besonders schützenswert. Raphael Krawietz, der Leiter des PDAG Rechtsdienstes meint dazu: «Eine patientenzentrierte Behandlung ohne funktionierenden Datenschutz ist nicht möglich. Der Datenschutz ist ein (Mindest-) Qualitätsmerkmal medizinischer Leistungen, denn hier geht es um die informationelle Selbstbestimmung.»

## Eine menschliche Firewall bilden

Nur, was bedeutet ein funktionierender Datenschutz für ein Spital? Zählt am Ende nicht einfach die Compliance gegenüber den kantonalen und nationalen Gesetzen? – Die Einhaltung der Gesetze, wobei für die PDAG die kantonale sowie die Bundesgesetzgebung Anwendung findet, ist tatsächlich ein wichtiger Treiber. Gerade das revidierte nationale Datenschutzgesetzt (revDSG), welches voraussichtlich Ende 2022 ohne Übergangsfrist in Kraft tritt, stellt die Organisationen vor grosse Herausforderungen. Für die PDAG bedeutet ein funktionierender Datenschutz aber weit mehr als das formelle Einhalten von Gesetzen. Es geht darum, den Datenschutz und die mit dem Datenschutz zwangsläufig verbundene Informationssicherheit täglich auf eine praxistaugliche Art und Weise zu leben. Werner Rykart, Leiter der PDAG Informatik, ist überzeugt: «Das grösste Risiko im Datenschutz- und der Informationssicherheit ist der Faktor Mensch. Entscheidend sind sensibilisierte Mitarbeitende, welche eine menschliche Firewall bilden.» – Mit dieser Überzeugung hat die PDAG im vergangenen Jahr ein ganzheitliches Datenschutz- und Informationssicherheits-Managementsystem (DSMS/ISMS) aufgebaut.

## Klares Verständnis von «Managementsystem»

Selbstverständlich haben sich die PDAG auch in der Vergangenheit um den Datenschutz und die Informationssicherheit gekümmert. Gerade in der IT-Sicherheit sind die PDAG mit ihrem professionellen IT-Provider, der HINT AG, seit Jahren hervorragend aufgestellt. Ausdruck dieser Professionalität ist die ISO 27001-Zertifizierung der HINT AG. Mit dem aufgebauten Managementsystem katapultieren sich die PDAG in eine neue Sphäre des Datenschutzes und der Informationssicherheit hoch. Dies bedeutet insbesondere: Die PDAG geht weg von punktuellen Einzelmassnahmen und hin zu systematisch gesteuerten Massnahmen in Sinne des Deming-Kreislaufes; auf Basis einer fassbaren Datenschutz- und Informationssicherheitsstrategie. Isoliertes Wissen von Einzelper-

Die Psychiatrischen Dienste Aargau haben Pionierarbeit geleistet in Sachen Datenschutz. Unser Bild zeigt eine Impression des Hauptsitzes in Königsfelden.

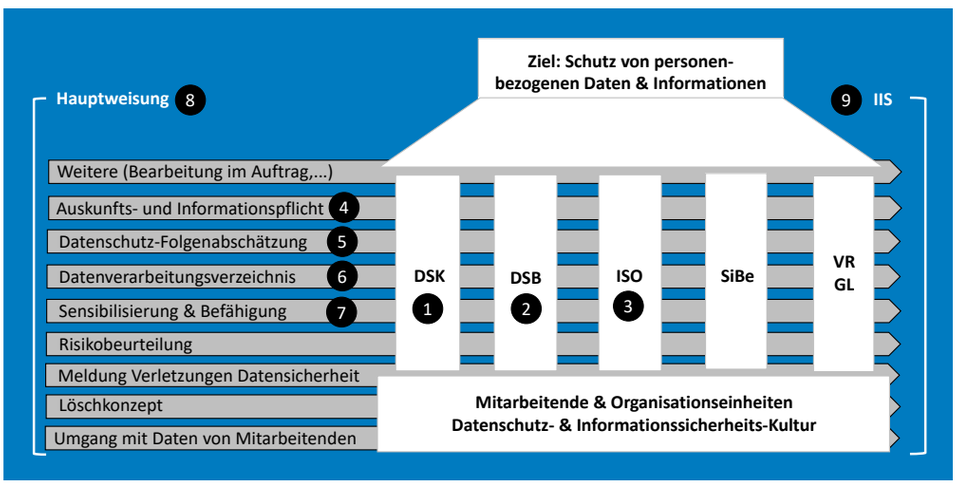
sonen im Rechtsdienst und der Informatik wurde durch aktiv vernetztes Wissen über alle Bereiche und Kliniken ersetzt.

Das bedeutet, dass nicht geregelte Aufgaben, Kompetenzen und Verantwortlichkeiten von nun an klar definiert sind. Dezentrale und abteilungsbezogene Dokumentenablagen wurden zentralisiert und nachvollziehbar geregelt. Zweck Sensibilisierung aller Mitarbeitenden führt die PDAG neu obligatorische Schulungen durch. Die teilweise dem Zufall überlassene Zusammenarbeit mit den zuständigen Behörden wich einer bewussten Kooperation; im Sinne einer vertrauensbildenden Zusammenarbeit.

Das PDAG Datenschutz- und Informationssicherheits-Managementsystems enthält viele wichtige Elemente. Das Framework gliedert sich dabei in drei Bereiche:

1. Die Aufbauorganisation resp. die Organe des Datenschutzes und der Informationssicherheit (1 bis 3)
2. Die Ablauforganisation resp. die Prozesse des Datenschutzes und der Informationssicherheit (4 bis 7)
3. Die Klammern, welche Aufbau und Ablauforganisation zusammenhalten (8 und 9)

Abb. 1




## Aufbauorganisation Datenschutz und Informationssicherheit

(in Abb. 1 der Tempel)

### 1. Datenschutzkommission (DSK)

Seit Ende 2020 ist die gesetzlich nicht vorgeschriebene DSK operativ tätig, d.h. die PDAG betreibt die DSK aus Überzeugung. Die DSK wird vom Leiter Rechtsdienst und dem Leiter Informatik geführt. Alle Kliniken und Bereiche haben Einsitze in die DSK, deren Mitglieder als «Brückenbauer» zwischen dem «theoretischen Datenschutz» und der «Praxis» agieren. Die DSK hilft den Datenschutz praxis- und alltagstauglich in der PDAG umzusetzen. Hierzu gibt sie Empfehlungen zu Datenschutz-Folgenabschätzungen, Datenschutzweisungen und -schulungen zu Handen der Geschäftsleitung ab. Sie unterstützt den Datenschutzberater/die Datenschutzberaterin, wenn Massnahmen im Zuge von Meldungen betreffend der Verletzung der Datensicherheit ergriffen werden müssen. Die DSK rapportiert jährlich direkt dem CEO.

### 2. Datenschutzberater/ Datenschutzberaterin (DSB)

Der/die DSB überwacht die Einhaltung der Datenschutzvorschriften innerhalb der PDAG. Er/Sie ist für die juristische Beantwortung von datenschutzrechtlichen Fragen – gegebenenfalls in Zusammenarbeit mit dem Rechtsdienst – zuständig. Er/Sie überprüft gleichfalls die Konformität des DSMS und berät die Geschäftsleitung in Datenschutzbelangen. Der/die DSB übt die Funktion fachlich unabhängig aus und ist betreffend seiner/ihrer Funktion nicht weisungsgebunden. Folgende Aufgaben gehören u.a. zu den Aufgaben des/der DSB:

- Begleitet die Durchführung von Datenschutz-Folgenabschätzungen
- Sicherstellung der Bewirtschaftung des Datenverarbeitungsverzeichnisses
- Bearbeitung von Meldungen über Verletzungen der Datensicherheit.
- Sicherstellung des Auskunftsrechtes
- Durchführungen von Datenschutzschulungen gemäss Schulungskonzept
- Vertragliche Sicherstellung/Prüfung von Verträgen bei Auftragsdatenbearbeitung (Outsourcing)
- Durchführung von Kontrollen betreffend die Umsetzung des Datenschutzes
- Reporting: Regelmässige Information des CEO, Erstellung des Jahresberichts zuhanden der Geschäftsleitung und der Datenschutzkommission.

### 3. Information Security Officer (ISO)

Auch die Funktion des ISO wurde in der PDAG neu geschaffen und wird aktuell auf Mandatsebene besetzt. Der Fokus des ISO liegt auf der Informationssicherheit. Zusammenfassend lässt sich sagen, dass der/die ISO die interne/externe Informatik überwacht und Risiken identifiziert, bewertet und behandelt. Der/die ISO ist in die Kontrollen von internen und externen Vorgaben eingebunden, ist Mitglied der Datenschutzkommission und ist analog zum/zur DSB in der Ausübung der Funktion fachlich unabhängig.

## Ablauforganisation Datenschutz und Informationssicherheit

(in Abb. 1 die Pfeile)

### 4. Auskunfts- und Informationspflicht

Die PDAG gewährleistet durch Weisungen die Auskunfts- und Einsichtsrechte gemäss der Datenschutzgesetzgebung für Patienten, Mitarbeitende und Dritte.

### 5. Datenschutz-Folgenabschätzung

Wird eine neue personenbezogene Datenbearbeitung eingeführt, z.B. die Implementierung einer neuen Software, muss vorab geklärt werden, ob die beabsichtigte Datenbearbeitung voraussichtlich die Persönlichkeit oder die Grundrechte der von der Bearbeitung betroffenen Personen beeinträchtigen kann. Im Falle einer möglichen Betroffenheit wird unter der Federführung des/der Datenschutzberaters/in eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt. Ergibt die DSFA, dass durch die beabsichtigte Datenbearbeitung ein erhöhtes Risiko für die Persönlichkeit oder die Grundrechte besteht, muss entweder die eidgenössische oder die kantonal beauftragte Person für Datenschutz und Öffentlichkeit (ÖDB) konsultiert werden, welche dann Empfehlungen zur Umsetzung der Datenbearbeitung abgeben kann.

### 6. Datenverarbeitungsverzeichnis

Voraussetzung für einen funktionierenden Datenschutz ist die Kenntnis darüber, wo, von wem und zu welchem Zweck, aufgrund welcher Grundlage personenbezogene Datenbearbeitungen vorgenommen werden. Aus diesem Grund führt die PDAG ein Verzeichnis über die Bearbeitungstätigkeiten im Sinne von Art. 11 des Bundesgesetzes über den Datenschutz (revDSG) vom 25. September 2020. Der Inhalt dieses Verzeichnisses ist:
a. Identität des Verantwortlichen

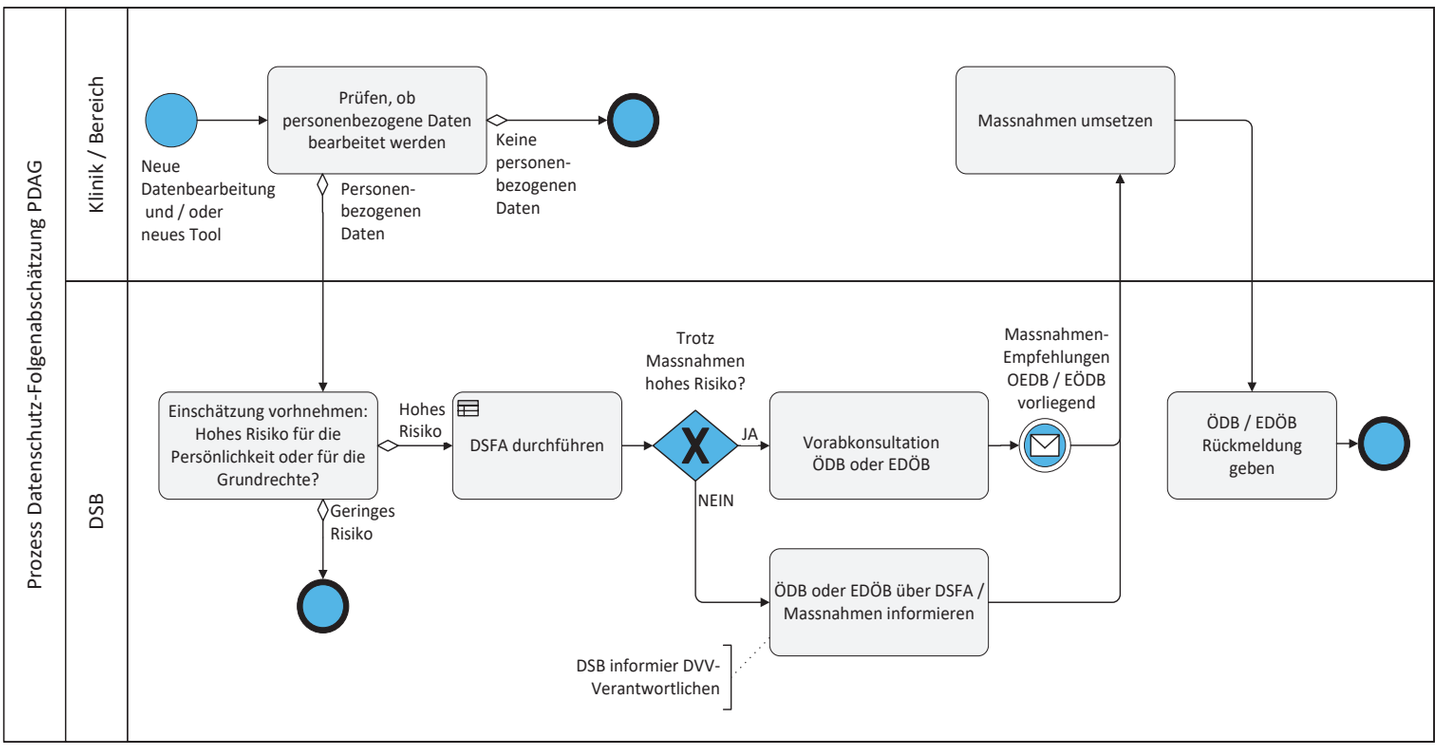
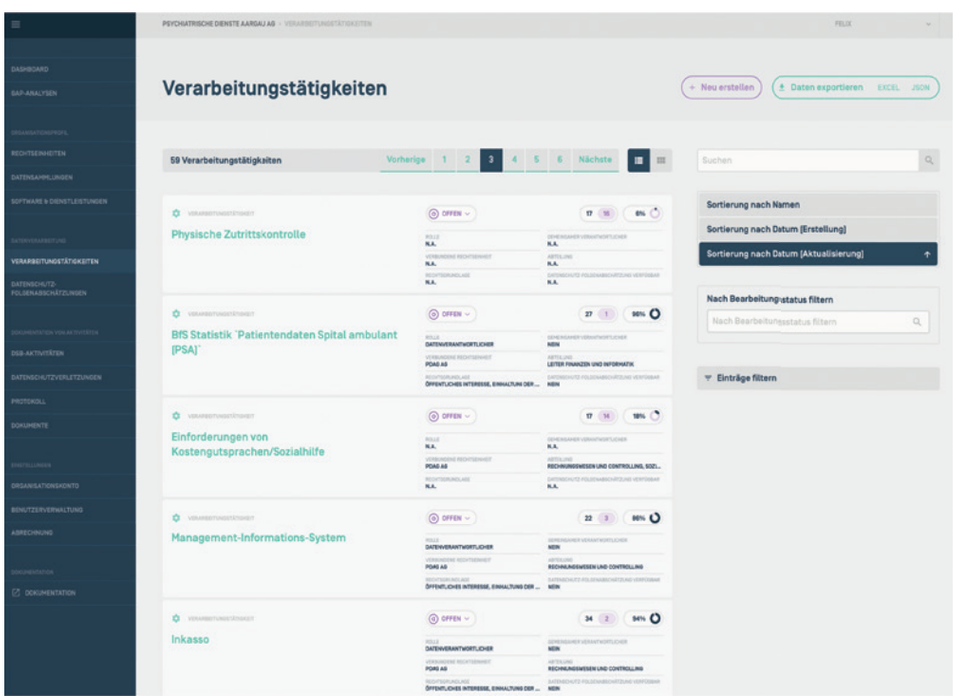



Abb. 2

b. Bearbeitungszweck
c. Beschreibung der Kategorien betroffener Personen (z.B. Patientinnen und Patienten, Mitarbeitende etc.)
d. Kategorien der betroffene Personendaten (z.B. besonders schützenswerte Personendaten)
e. Kategorien der Empfänger (z.B. Behörden usw.)
f. Aufbewahrungsdauer (wenn möglich) oder Kriterien, nach welchen sich die Aufbewahrungsdauer richten (vgl. Zusammenhang zu «Bearbeitungszweck»).
g. Gesetzliche Grundlage bzw. Beschreibung des überwiegenden Interesses, auf deren Basis die Bearbeitungen erfolgen.
h. Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit (wenn möglich)
i. Allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit.

Die PDAG konnten durch die auf Datenschutzrecht spezialisierten Anwälte Lukas Bühlmann und Marco Meier (MLL Meyerlustenberger Lachenal Froriep AG) kompetente Partner finden, um zunächst die Anforderungen an ein Datenverarbeitungsverzeichnis, welches auf die PDAG zugeschnitten ist, zu definieren. Die anschliessende unternehmensweite Erfassung der Datenverarbeitungen erfolgte dann durch ein interdisziplinäres Team unter der Führung eines Projektleiters der Unternehmensentwicklung, der IT und dem Rechtsdienst. Die Erhebung der Datenverarbeitungen gleicht einer Herkules-Aufgabe und ist nach der Erfahrung der Projektverantwortlichen der PDAG mit Standard-Office-Tools nicht übersichtlich zu bewerkstelligen. Die PDAG hat daher 2020 eine Software-Evaluation durchgeführt und setzen heute zur Bewirtschaftung des Datenverarbeitungsverzeichnisses die spezialisierte Software ZOA ein.

Abb. 3




Eine «High Level» Spiegelung des Datenverarbeitungsverzeichnisses ist auf der Website der PDAG abrufbar. Hier weisen die PDAG allen Interessierten transparent aus, zu welchen Zwecken und mit welcher gesetzlichen Legitimation sie personenbezogene Daten bearbeiten: www.pdag.ch/ueber-die-pdag/umgang-mit-personendaten/

**7. Sensibilisierung und Befähigung**
Die PDAG investieren im laufenden Jahr viel Zeit und Geld in die Schulung der Mitarbeitenden, Awarness-Trainings und interne Audits. Der Schwerpunkt liegt hier bei der Informations- resp. der IT-Sicherheit. Hier identifizieren die PDAG eines ihrer grössten Betriebsrisiken. Als Grundschulung wurde deshalb ein professionelles E-Learning eingeführt.

- Missbrauch und Kontrollen
- Sanktionierung

Einer der wichtigsten Faktoren, dass das DSMS/ISMS nicht als auf «dem Reissbrett erstelltes Dokument» verkümmert, ist die Kunst, dem Ganzen «Leben einzuhauchen». Dieses «Einhauchen» gelingt, indem die Mitarbeitenden motiviert werden, selbst die Datenschutzthematiken


## Zentrale Weisungen für die Aufbau- und Ablauforganisation

(in Abb. 1 die Klammern)

**8. und 9. Hauptweisung Datenschutz und Weisung betreffend die Informations- und Informatiksicherheit (IIS)**
Die Hauptweisung betreffend den Datenschutz und die Weisung betreffend die Informations- und Informatiksicherheit sind die zentralen Weisungen, welche Aufbau- und Ablauforganisation des DSMS/ISMS zusammenhalten. Besonders die IIS hat einen täglichen Impact auf die Mitarbeitenden. Hier sind folgende Regeln definiert:

- Grundsätze zur Nutzung der Informatikmittel
- Zugangs- und Zugriffsschutz
- Umgang mit Personendaten (Datenablage, Drucken und Scannen, Stellvertretende Zugriffe, Cloud Computing, Sicheres Löschen von Daten).
- Schutz bei der Datenübermittlung (E-Mail und Internet)
- Sicher und mobil unterwegs
- Umgang mit Geräten und Einrichtungen im Informatikumfeld

zu erkennen. Die PDAG konnten bereits in der Projektphase erfahren, wie immer mehr Mitarbeitende für die Thematik sensibilisiert waren und sich aktiv einbrachten. Sie erkannten, dass die Thematik Datenschutz nicht ein abstraktes rechtliches Thema ist, sondern es sich um praktische Fragen handelt, mit welchen sie täglich konfrontiert sind. Es steht daher für die PDAG ausser Frage, dass die Basis des Datenschutz, die Mitarbeitenden, durch regelmässige Schulungen im Datenschutz weitergebildet werden.

## Lessons Learned zum Aufbau des DSMS/ISMS

Heiner Reichlin, Vizepräsident des Verwaltungsrats der PDAG und Mitglied im Soundingboard betont: «Angriffe auf Daten und Informationen erfolgen heute fast ausschliesslich über den Weg des ‹social engineering›. Die Aufklärung und Schulung unserer Mitarbeiter zu ‹awareness› hat deshalb für die PDAG höchste Priorität.» Und Felix Schaub, Projektleiter, ergänzt: «In der PDAG konnte dieses Herkules-Projekt dank drei Faktoren in nur einem Jahr durchgezogen werden:

1. Das starke Commitment des Top-Managements war während des ganzen Projekts spürbar. Das ist nach meiner Erfahrung in solchen Fleissprojekten nicht selbstverständlich.
2. Wir verfügten über eine hervorragend funktionierende Projektorganisation, dank Mitgliedern mit einer hohen Arbeitsdisziplin. Das tönt unspektakulär, ist aber entscheidend.
3. Der Blick über den Tellerrand – Input von Extern: Einerseits wurde das Projekt durch die VAKA (Branchenverband der Aargauer Spitäler, Kliniken und Pflegeinstitutionen) begleitet. Die VAKA betreibt eine Fachstelle für Datenschutz und koordiniert die Umsetzung des kantonalen Datenschutzgesetztes (IDAG) im Kanton Aargau. Anderseits verglichen wir unsere Arbeit immer wieder mit anderen Spitälern, welche auf diesem Gebiet führend sind. Das half enorm.»

## Interdisziplinäre Qualitäten sind gefragt

Hans Urs Schneeberger, Geschäftsführer VAKA und Mitglied Soundingboard bestätigt denn auch: «Der Datenschutz in der PDAG ist professionell aufgebaut und sehr weit fortgeschritten.» Auf einen besonders wertvollen Erfolgsfaktor weist Raphael Krawietz, Leiter Rechtsdienst und Mitglied Projektteam, hin: «Die Thematik des Datenschutzes und der Informatiksicherheit ist derart komplex, dass ausschliesslich ein interdisziplinärer Ansatz erfolgsversprechend ist. Das haben wir alle gelernt und ich bin stolz darauf, wie wir über die Abteilungsgrenzen zusammengerückt sind.»

Gabi Hilpert, Stv. Leiterin HR und Mitglied Projektausschuss stimmt voll und ganz zu: «Das bisher leidige Thema Datenschutz!? Mit einem tollen, interdisziplinären und motivierten Team bereitete es sogar ‹Spass›, diese Meilensteine zu setzen.» Werner Rykart, Leiter Informatik und Mitglied Projektteam meint zusammenfassend: «Mit der Digitalisierung und Vernetzung von Diensten und Produkten steigt auch die Bedeutung des Datenschutzes. Das wurde besonders mit Beginn der Anwendbarkeit der DSGVO im Jahr 2018 sichtbar.»

## IT-Sicherheit ist nicht automatisch Datenschutz

«Die Gleichsetzung von IT-Sicherheit und Datenschutz führt häufig zu einem folgenschweren Missverständnis: Wenn die Unternehmensleitung glaubt, alles Notwendige für die IT-Sicherheit getan zu haben, meint sie damit oft auch

den Anforderungen des Datenschutzes zu genügen. Oft wird jedoch verkannt, dass IT-Sicherheit nur teilweise mit dem Datenschutz deckungsgleich ist», führt Werner Rykart weiter aus: «Abgesehen davon, dass die IT-Sicherheit die gesamte (auch nichtpersonenbezogene) Datenverarbeitung betrifft, muss sich erst ein «Gespür» dafür herausbilden, dass Massnahmen zur IT-Sicherheit nicht per se datenschutzkonform oder gar datenschutzfreundlich sind. Vielmehr bedarf es dazu einer Analyse und Bewertung der möglichen Massnahmen zur Feststellung und Abwehr von sicherheitsrelevanten Vorfällen. Dank der guten Zusammenarbeit aller Beteiligten wird dies heute in der PDAG sichergestellt.»

### Weitere Informationen

Felix.Schaub@pdag.ch (Projektleiter)
www.pdag.ch

Felix Schaub, Projektleiter Unternehmensentwicklung Psychiatrische Dienste Aargau AG

### Die Psychiatrischen Dienste Aargau

Die Psychiatrischen Dienste Aargau (PDAG) gewährleisten die psychiatrische Behandlung und Betreuung mit Notfalldienst und Krisenintervention für die Kantonsbevölkerung.

Massgeschneiderte stationäre und ambulante sowie konsiliarische Angebote bestimmen die Behandlungsart, die individuell zu Betroffenen, ihrer Krankheit und Lebenssituation passt. Die Leistungen werden in den vier Kliniken (Klinik für Kinder- und Jugendpsychiatrie und Psychotherapie, Klinik für Psychiatrie und Psychotherapie, Klinik für Forensische Psychiatrie, Klinik für Konsiliar-, Alters- und Neuropsychiatrie) und 14 ambulanten dezentralen Einrichtungen erbracht.

Seit 2004 sind die PDAG eine Aktiengesellschaft im Eigentum des Kantons Aargau. Für die PDAG arbeiten rund 1400 Personen in über 50 Berufen. Die PDAG sind Lehrspital der Medizinischen Fakultät der Universität Zürich und Ausbildungsstätte für Berufe im Gesundheitswesen.

Sie haben das Datenschutz- und Informationssicherheitskonzept massgeblich kreiert: von oben links nach rechts: Felix Schaub (Projektleiter), Dr. med. Heiner Reichlin (Vizepräsident VR PDAG), Dr. Hans Urs Schneeberger (Geschäftsführer vaka); von unten links nach rechts: lic.iur., LL.M. Raphael Krawietz (Leiter Rechtsdienst & Datenschutzberater PDAG), Werner Rykart (Leiter Informatik PDAG), Gabi Hilpert (Leiterin HR Business Partner/Stv. Leiterin Human Resources PDAG).