COMPLIANCE UND DIGITALISIERUNG

Die Digitalisierung stellt für Unternehmen, Behörden und Institutionen eine der aktuell größten Compliance-Herausforderungen dar. Die procilon Schriftreihe betrachtet unterschiedliche Aspekte dieses Wandels und gibt praxistaugliche Handlungsempfehlungen.

OZG

Jürgen Vogler
Andreas Liefeith

Inhaltsverzeichnis

Über Compliance

Der übergeordnete, englische Begriff Compliance lässt sich in seiner Bedeutung nicht wörtlich in die deutsche Sprache übersetzen. Insgesamt steht er für die Einhaltung von gesetzlichen Bestimmungen, regulatorischer und selbst gesetzter Standards sowie ethischer Regeln. Eine generelle gesetzliche Regelung für Compliance besteht nicht. Wesentliche Anforderungen lassen sich aber aus der deutschen Gesetzgebung und in zunehmendem Maß aus Verordnungen der Europäischen Kommission für den Binnenmarkt ableiten.

Damit gilt der Grundsatz, Compliance als Ganzes zu betrachten. Gerade dies hilft Geschäfts- und Verwaltungsprozesse so zu gestalten, dass Risiken bei der Digitalisierung minimiert werden.

Nur durch die Einbettung von Compliance-Maßnahmen in die tägliche Arbeit der Anwender entsteht so auch wirtschaftliche Nachhaltigkeit. Der Schutz von Informationen und Betriebsgeheimnissen im digitalen Zeitalter wird damit akzeptierter Bestandteil eines Ganzen und hilft Compliance-Anforderungen zu erfüllen.

Compliance-Herausforderung OZG

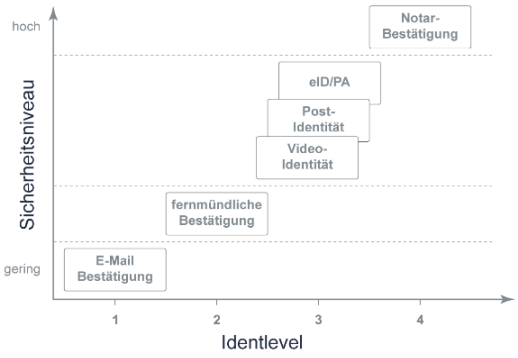
Die drei Seiten des **Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen** (OZG) legen sehr kurz die Rahmenbedingungen für die Digitalisierung in der öffentlichen Verwaltung fest. Mit der Zustimmung von Bundestag und Bundesrat sind deutschlandweit alle Behörden verpflichtet, spätestens am 31. Dezember 2022 alle Verwaltungsleistungen auch barriere- und vor allem medienbruchfrei elektronisch für Bürger und Unternehmen anzubieten.

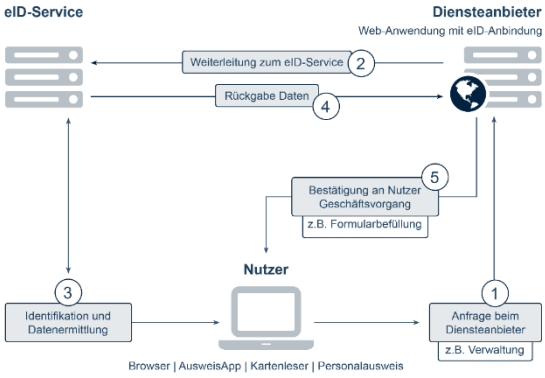
Im Gegensatz zum kurz gehaltenen Gesetzestext, lässt der fast 300-seitige OZG-Umsetzungskatalog erahnen, vor welcher großen Herausforderung Verwaltungen, aber auch IT-Dienstleister und Software-Hersteller stehen. Diese wird letztendlich nur durch ein hohes Maß an Standardisierung zu bewältigen sein.

Die Kernelemente

Sichere Identitäten

Explizit fordert der Gesetzgeber die Einrichtung von Nutzerkonten, welche, bezogen auf die jeweilige Nutzung einer Verwaltungsleistung, die Identität des Nutzers bestätigen. Das Wirkprinzip wird im Folgenden am Beispiel der eID-Funktion des Personalausweises dargestellt:



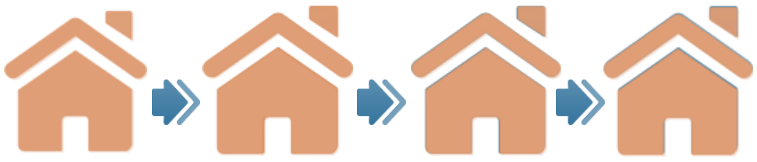


Da je nach Art der angebotenen Verwaltungsdienstleistungen auch unterschiedliche Sicherheitsniveaus zur Anwendung kommen können, kann somit auch bei der Identitätsbestätigung auf unterschiedliche Bestätigungsverfahren zurückgegriffen werden.

Auf den Nachweis der Identität auf unterschiedlichen Vertrauensniveaus oder sog. Identlevel wird im Gesetz unter § 8 Abs. (1) explizit hingewiesen.

Portalverbund

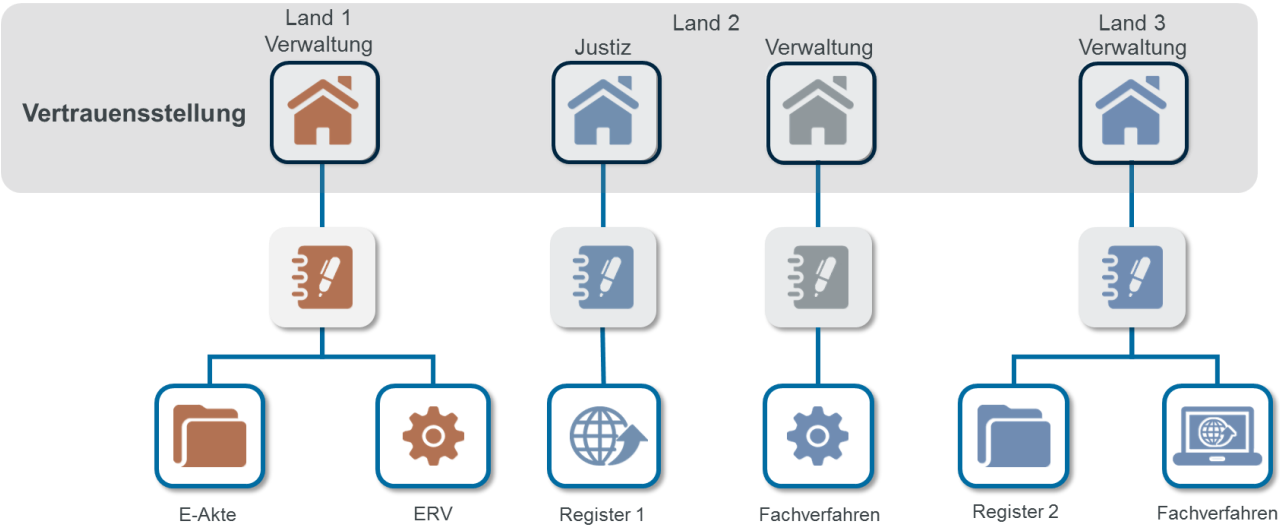
Durch den im Gesetz verankerten Begriff „Portalverbund“ soll es einem Nutzer möglich sein, unabhängig vom „Standort“ seines Benutzerkontos auf beliebige Verwaltungsdienstleistungen (V-DL) von Bund und Ländern zugreifen und nutzen zu können.



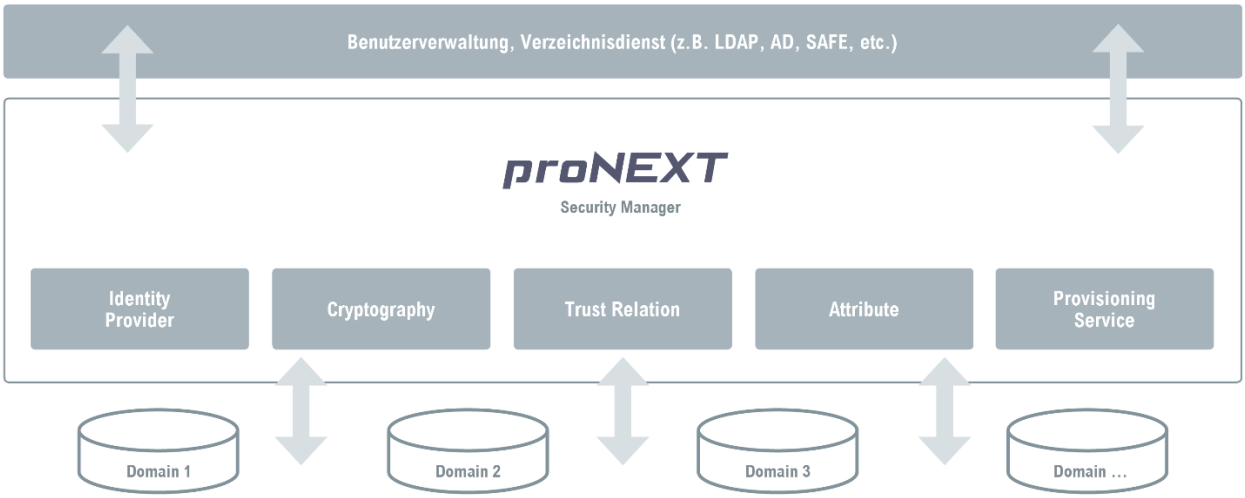
V-DL-Bund V-DL-Land 1 V-DL-Land 2 …

Damit stellt der Portalverbund eine technische Verknüpfung im Sinne eines Trusted-Domain-Konzeptes dar.

Durch die Festschreibung des Verbundes im Gesetz verfügen alle Verwaltungsportale damit untereinander über eine Vertrauensstellung. Eine Identität aus Domain Land 1 wird auch in anderen Domänen Land 2 + Land 3 als vertrauenswürdig betrachtet und Dienste können genutzt werden.

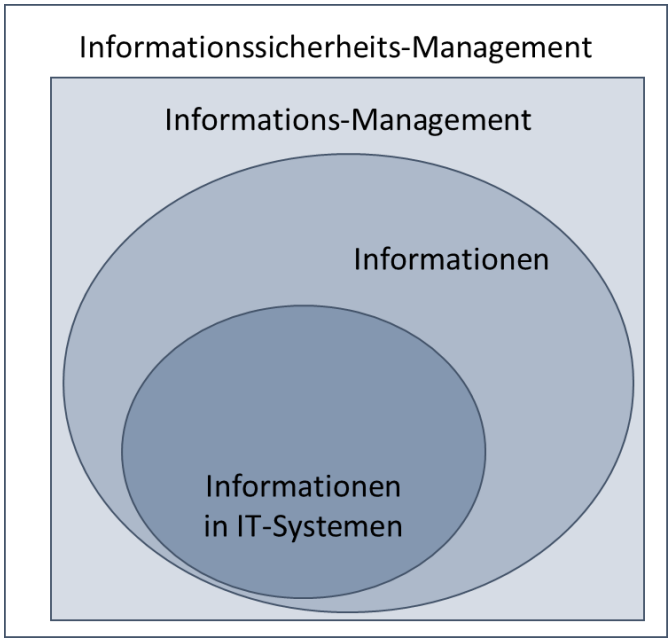


Moderne Software für Identity & Access Management (IAM) kann solche Szenarien problemlos über entsprechende Attribute in einem Rechte- und Rollenkonzept abbilden. Insbesondere die Integrationsfähigkeit der verwendeten IAM-Lösung in vorhandene Benutzerverwaltungen oder Verzeichnisdienste stellt dabei einen kritischen Erfolgsfaktor dar.



Informationssicherheit und Datenschutz

Erfreulicherweise wird im Gesetz die Einhaltung der IT-Sicherheit „für alle Stellen“ verbindlich festgeschrieben. Da eine Veränderung durch Landesrecht explizit ausgeschlossen wird, empfehlen sich für Verwaltungen als Arbeitsgrundlage der BSI-Grundschutz und die Implementierung der Informationssicherheit als Prozess im Sinne eines Informationssicherheitsmanagement-Systems (ISMS).



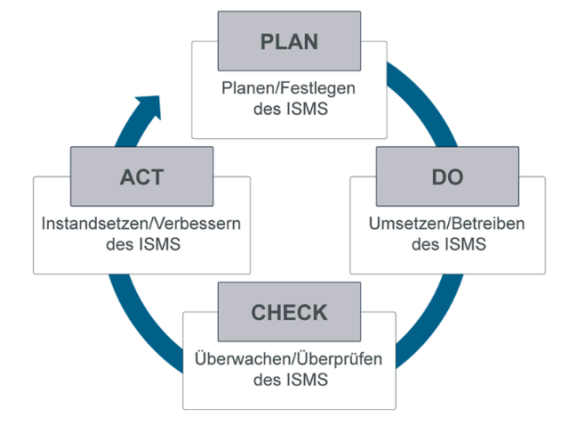
Nicht nur, aber vor allem im Zusammenhang mit dem Datenschutz wurde die Begrifflichkeit „technisch organisatorische Maßnahmen“ - kurz TOM - eingeführt.

Schon im BDSG der alten Fassung (a.F.) wurde in § 9 auf Maßnahmen zum Schutz personenbezogener Daten verwiesen.
In der aktuell gültigen DSGVO wird das Thema TOM in Art. 32 und BDSG (neu) im §64 ausführlich behandelt. Erfreulicherweise ist über den Verlauf der Zeit festzustellen, dass in der generellen Begrifflichkeit und der Systematik eine deutliche Annäherung zwischen Datenschutz und Informationssicherheit stattgefunden hat. Dennoch können die Gesetzestexte nicht alle Fragestellungen beantworten, die erforderlich sind, um Compliance für den Datenschutz herzustellen. Beispielhaft seien hier die Formulierung „Stand der Technik“ und Unterschiede bei der Risikobewertung genannt.

In einer zunehmend digitalen Welt liegt die Konvergenz von Informationssicherheit und Datenschutz auf der Hand. Auch die DSGVO basiert auf einem Risikomanagement zur Ableitung geeigneter TOM.

	Informationssicherheit	Datenschutz
Management ist verantwortlich (haftbar) für Umsetzung	X	X
Veröffentlichung von Leitlinien	X	X
Fortlaufende Kontrolle und Verbesserung	X	X
Bewertung von Risiken	X	X
Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit	X	X
Kontrolle von Lieferanten und Dienstleistern	X	X
Meldung von Vorfällen	X	X
Grundsatz Privacy/Security by design	X	X

Die geforderte zyklische Überprüfung des Datenschutzkonzeptes und der ergriffenen Maßnahmen entspricht dem PDCA-Zyklus in Management-systemen, die einen kontinuierlichen Verbesserungsprozess beinhalten (siehe ISO-Normen). Schlussfolgernd kann man also die Aktivitäten rund um die Datenschutz-Compliance auch als Datenschutz-Management-System (DSMS) bezeichnen.



PDCA-Zyklus im ISMS

Datenschutz-Management-System (DSMS)

Auch finden sich in der DSGVO die klassischen Schutzziele der Informationssicherheit **Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität** wieder.

Zusätzlich führt die DSGVO den Begriff der Belastbarkeit hinsichtlich verwendeter Systeme und Dienste ein. Da dies im Weiteren nicht genauer beschrieben ist, liegt eine Interpretation des Begriffes für den Praktiker als Bestandteil der Verfügbarkeit nahe.

Aus der Praxis

Identitätsmanagement im Elektronischen Rechtsverkehr

Federführend für den reibungslosen Ablauf des ERV ist die Bund-Länder-Kommission für Informationstechnik (BLK) in der Justiz. Als Kern werden hier die Standards für die bewährten Infrastrukturkomponenten zur sicheren Kommunikation per Ende-zu-Ende-Verschlüsselung, integrierte Quittungsmechanismen, Prüfprotokolle und die Benutzerverwaltung (Verzeichnisdienst SAFE) definiert und weiterentwickelt.

Die Infrastruktur wird für Nutzer, wie z.B. Firmen, Behörden oder auch Bürger, von der Justiz zur Verfügung gestellt. Voraussetzung ist eine ERV-konforme Sende- und Empfangssoftware.

Grundlegendes Element für den ERV ist eine elektronische Identität durch die Registrierung im sicheren Verzeichnisdienst nach dem SAFE-Standard. Hier wurde mit dem ‚Virtuellen Attributs Service' eine Komponente implementiert, die nach dem Trusted-Domain-Konzept Vertrauensstellungen unterschiedlicher Gruppen wie Gerichte, Rechtsanwälte, Notare oder auch Behörden herstellt. Gesicherte Zugriffe und Kommunikation werden damit domainübergreifend mit nur einer Registrierung möglich.

Sicheres Zugriffsmanagement „OPEN BANKING"

Um das Zusammenspiel von unterschiedlichen Systemen und Applikationen zu veranschaulichen, sei hier auf die Grundelemente des ‚Open Banking' und die dort definierte PSD2 – KONTOSCHNITTSTELLE verwiesen.

Banken müssen bei onlinefähigen Zahlungskonten offen dokumentierte Schnittstellen bereitstellen, die es einem Third Party Provider (TPP) erlaubt, im Kundenauftrag auf Kundenkonten zuzugreifen. Dies dient letztendlich der Bestätigung der Verfügbarkeit eines Geldbetrags zur Bezahlung einer Transaktion. TPP erhalten in Echtzeit unmittelbaren Zugang zu sämtlichen Kontoinformationen des Kunden. Zahlungs-anweisungen werden vom TPP elektronisch und im Namen des Kunden vorgelegt.

Damit diese Zugriffe ein hohes Maß an Informationssicherheit erfüllen, ist eine Reihe von Maßnahmen vorgeschrieben. Dazu gehören:

- gesicherte elektronische Kommunikation zwischen Bezahl-App und kontoführender Bank

- Zwei-Faktor-Authentifizierung (2FA) mit zwei Authentifizierungs-elementen aus den Kategorien Wissen, Besitz und Inhärenz
- Dynamic Linking - Authentication-Code ist bei Fernzugriff dynamisch mit Betrag und Empfänger der Zahlung verknüpft
- Separated Execution Environment - auf Smartphones ist eine sichere Ausführungsumgebung zu verwenden

Ein Zahlungsdienstleister muss sich für jeden Zugriff auf ein Konto mittels qualifizierter Zertifikate gemäß eIDAS (qualifizierte Webseiten-Zertifikate und Siegel) identifizieren. Die Identifizierung des Zertifikatsinhabers erfolgt durch einen Vertrauensdienste-Anbieter (VDA), der u.a. die Sperrung von Zertifikaten und deren Erweiterung durch spezifische Attribute sicherstellt.

Die Analogien zu lt. OZG einheitlichem Zugriff auf beliebige Verwaltungs-dienstleistungen liegen auf der Hand.

Der DSMS-Zyklus

Schutzbedarf personenbezogener Daten

Generell kann bei der Schutzbedarfsfeststellung von praxiserprobten Vorgehensmodellen der Informationssicherheit profitiert werden. Der Fokus liegt natürlich an dieser Stelle auf den personenbezogenen Daten. Für diese wird eine Einstufung in die Kategorien „normal“, „hoch“ oder „sehr hoch“ getroffen werden müssen, denn letztendlich leiten sich daraus später die TOM ab.

Risikobewertung

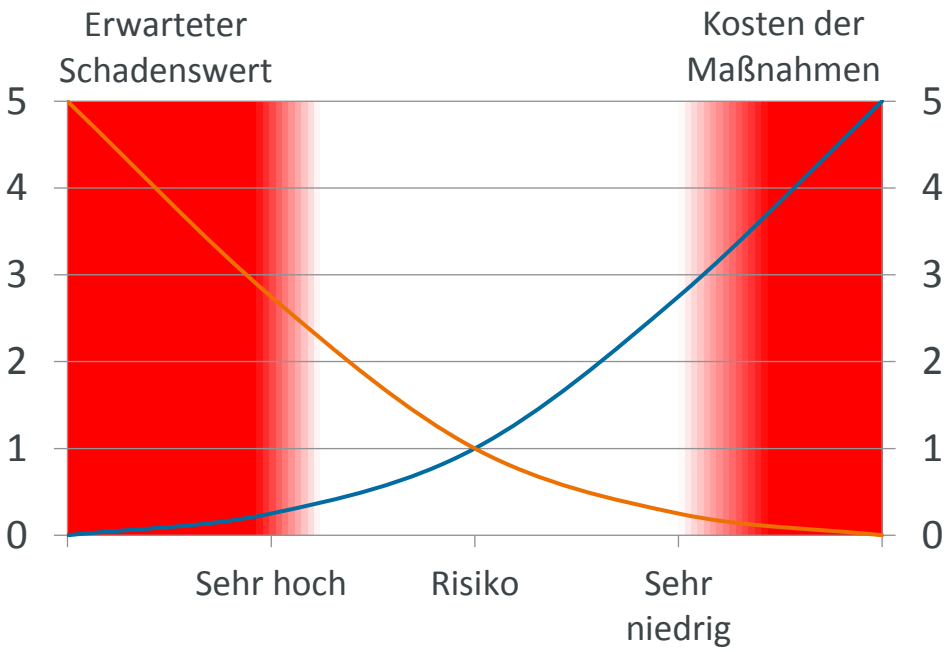
Auch für die Risikobewertung finden sich Analogien in der Informations-sicherheit. Allerdings sind bei der Bewertung der Eintrittswahr-scheinlichkeit im Zusammenhang mit dem Datenschutz wesentliche Unterschiede zu beachten.

Die Informationssicherheit betrachtet aus der Sicht des Unternehmens relevante Informationswerte. Der Datenschutz umfasst zusätzlich die Rechte Dritter, welche zu wahren sind. Neben der Schwere des Risikos für die Rechte und Freiheit natürlicher Personen, rücken die Risiken für betroffene Personen in den Mittelpunkt. Betroffene Personen können auch Externe (z.B. Kunden, Lieferanten, Partner, Patienten, etc.) sein.

Technische und organisatorische Maßnahmen

Werden an diesen Stellen genaue Handlungsempfehlungen erwartet, so fallen erst einmal zwei Begriffe auf, die dies verhindern. In einem Satz zusammengefasst ist von „geeigneten“ Maßnahmen nach „Stand der Technik“ die Rede. Kritiker sehen hier zu viele Schlupflöcher. Auf der

anderen Seite ist nachvollziehbar, dass der Gesetzgeber keine technischen Maßnahmen in eine Verordnung schreibt, die ggf. bei Inkrafttreten überholt sind. Für die Festlegung geeigneter Maßnahmen sind die bereits durchgeführte Risikoanalyse und vor allem die Ermittlung des Schutzbedarfs die elementare Grundlage. Generell sollte man zur Bestimmung der „Eignung“ einen risikooptimierten Ansatz gemäß folgender Betrachtung wählen:



Zum „Stand der Technik“ hat sich inzwischen eine unter Federführung des IT-Sicherheits-Verbandes TeleTrusT entstandene Publikation bewährt. Diese wird zyklisch aktualisiert und procilon ist von Anfang an Mitautor.

Nach Betrachtung der unterschiedlichen Aspekte entsteht letztendlich ein Maßnahmenkatalog, der im Wesentlichen folgende Aspekte enthält:

- technische Maßnahmen zur physischen Sicherheit (Zäune, Schlösser, bauliche Maßnahmen)
- technische Maßnahmen durch Hardware
- technische Maßnahmen durch Software
- organisatorische Maßnahmen (Mitarbeiterschulungen, Arbeitsanweisungen, Besuchermanagement)

Nachweis der Konformität

Hier treffen wir auf die grundlegende Absicht dieses Dokumentes. Es geht um die Einhaltung von Compliance im Datenschutz, also den Vergleich zwischen Soll- und Istzustand. Und genau hier tritt ein ähnliches Problem wie bei dem TOM auf, denn ein eindeutiger, prüfbarer Istzustand ist bisher nicht definiert. Zwar zeichnen sich auch hier einige Parallelen zur Informationssicherheit ab, aber eine objektive Zertifizierungsmethode existiert nicht.

Fazit

Verwaltungsmodernisierung als Ziel des Gesetzgebers

Die vorgeschriebene Umsetzung des Onlinezugangsgesetzes (OZG) bis zum 31.Dezember 2022 stellt die Verwaltungen von Bund, Ländern und Kommunen durchaus vor bedeutende Herausforderungen. Dies begründet sich nicht nur aus dem gesetzten rechtlichen Rahmen des OZG selbst, sondern darüber hinaus aus der Einhaltung bestehender und zu erwartender Gesetze. Das eigentliche Ziel des Gesetzgebers, die digitale Verwaltungsmodernisierung Deutschlands, kann nur erreicht werden, wenn parallel zu den technischen Aspekten das Potential völlig neu gedachter digitalisierter Prozesse ausgeschöpft wird. Hier verbirgt sich bei den 575 Verwaltungsleistungen, die im Rahmen der Umsetzung des OZG bis Ende 2022 online angeboten werden müssen, sicher noch ein erhebliches Innovationspotential.

Automatisierung & Verwendung digitaler Identitäten

Zentraler Baustein zum Ausschöpfen der Digitalisierungspotenziale wird die Verwendung sicherer – verifizierter – digitaler Identitäten sein. Mit ihnen bietet sich die Chance auch Verwaltungsleistungen umfangreich zu automatisieren und eine vertrauenswürdige Kommunikation zwischen Bürger und Unternehmen mit den Verwaltungen zu gewährleisten. Das gleiche trifft für den automatisierten Datenaustausch zwischen Systemen (m2m) innerhalb der Verwaltungen zu. Hierbei ist auf der einen Seite eine große Herausforderung für die Hersteller von Fachsoftware zu erkennen. Auf der anderen Seite ergibt sich die große Chance völlig neue Prozesse und Applikationen zu entwickeln und zu implementieren.

In der Praxis des elektronischen Rechtsverkehrs (ERV) sind solche Szenarien mit dem SAFE-Verzeichnisdienst und den besonderen elektronischen Postfächern für Behörden, Notare und Rechtsanwälte bereits heute im Einsatz. Ein wertvoller Erfahrungsschatz, der auch für die Umsetzung des OZG nutzbar ist.

Im Sinne eines standardisierten Identity- & Access Managements bieten sichere elektronische Identitäten die Chance, Single-Sign-on Implementierungen im Rahmen des geplanten Portalverbundes zwischen Kommunen, Landes- und Bundesbehörden einfach, effektiv und sicher zu realisieren. Mit der eIDAS-Verordnung ist dafür ein europaweit gültiger Standard gesetzt. Nun gilt es, diesen praxistauglich anzuwenden.

Mit dem fachlichen Knowhow rund um Datenschutz und Informations-sicherheit, insbesondere zur Anwendung sicherer elektronischer Identitäten arbeitet auch procilon gemeinsam mit Kunden und Anwendern an der Beantwortung der vielen offenen Fragen mit.

Die Autoren

Jürgen Vogler

Geschäftsführer der procilon IT-Solutions GmbH

Herr Vogler verfügt über mehr als 20 Jahre Erfahrung als Geschäftsführer, Berater und Consultant - vorwiegend in den Branchen Public und HealthCare. In diesen Branchen hat Herr Vogler Projekte durchgeführt und geleitet, sowie umfangreiche strategische Projekte mit den Kunden verantwortet.

Thematisch ist Herr Vogler neben dem Informatiker für Medizinökonomie vor allem im Umfeld der sicheren elektronischen Kommunikation, Signaturen, TrustCenter, eIDAS, Datenschutz und Datensicherheit und korrelierenden Themen bekannt. Nachdem Herr Vogler bei Mummert + Partner (heute Sopra Steria Consulting) im Marktcenter Public erfolgreich bis 2007 tätig war, wechselte er in 2007 in den Services Bereich der Microsoft Deutschland. Im Jahre 2009 wechselte er zur adesso AG, um dort im Business Development die Branche „Public“ neu für die adesso zu erschließen. Danach wechselte Herr Vogler 2011 zur Francotyp Postalia AG, wo er zunächst das Geschäftsfeld eBusiness leitete, bevor er bei dem Tochterunternehmen Mentana Claimsoft die Geschäftsführung übernahm. Begleitend zu diesem beruflichen Werdegang war Herr Vogler seit 2009 auch selbständig tätig. Hier vor allem als gefragter Experte zu den Themen der sicheren Kommunikation, Machbarkeit und strategische Beratung, aber auch als Interimsmanager und Keynote Speaker.

Herr Vogler verfügt über ein großes Netzwerk und ist im Vorstand der Kommune 2.0 und von buergerservice.org.

Andreas Liefeith

Leiter Marketing, procilon GROUP

Geboren 1961, schloss Herr Liefeith 1986 sein Studium an der Technischen Universität Dresden als Diplomingenieur für Elektrotechnik ab. Von 1986-1990 war er im VEB Uhrenwerk Ruhla tätig. Von 1990 bis 2012 war Herr Liefeith Mitarbeiter der IBM Deutschland GmbH. Anfangs in der Niederlassung Erfurt und später in Leipzig.

Seit dem Jahr 2012 verantwortet er das strategische Marketing der procilon Unternehmensgruppe.

Technologie für Informationssicherheit und Datenschutz

www.**procilon.de**

procilon GROUP GmbH
Leipziger Straße 110 04425 Taucha

Kontakt:

+49 34298 4878-31 | anfrage@procilon.de