ITEBO
Unternehmensgruppe
ganz nah

Ausgabe 2 | 2022

Datenschutz Spezial

Sonderausgabe – Datenschutz

Titelthema
Von unscheinbar bis unverzichtbar
ITEBO berät seit 16 Jahren zum Thema Datenschutz und IT-Sicherheit

Portfolio
Datenschutz und IT-Sicherheit
Ähnlich, aber doch ganz anders

Von Haus aus
Kommunale Fachanwendungen und Datenschutz
Einführungsprojekte ganzheitlich gedacht

Inhaltsverzeichnis

Impressum

ITEBO ganz nah
Das Magazin der ITEBO-Unternehmensgruppe

Herausgeber
ITEBO GmbH
Dielingerstraße 39/40
49074 Osnabrück
Tel.: 0541 9631-0
info@itebo.de · www.itebo.de

Verantwortlich für den Inhalt gemäß
§ 5 Telemediengesetz (TMG): Bernd Landgraf

Redaktion
ITEBO-Unternehmensgruppe

Konzeption, Layout
b2 Werbeagentur, Braunschweig

Texte
Sarah Kreilaus, ITEBO

Umschlagfoto
©stock.adobe.com/Fractal Pictures, VideoFlow

Druck
Individual.Druck, Osnabrück

Erscheinungsweise/Auflage
dreimal jährlich, 2000 Exemplare

Bernd Landgraf, Geschäftsführer
ITEBO-Unternehmensgruppe

ITEBO Unternehmensgruppe ganz nah

Datenschutz und IT-Sicherheit gewinnen immer mehr an Bedeutung

Die regelmäßigen Leserinnen und Leser unseres Kundenmagazins wissen, dass wir besondere Schwerpunkte in den Mittelpunkt jeder Ausgabe stellen. Diesmal wurde von unserem Redaktionsteam das Thema Datenschutz und IT-Sicherheit gewählt.

Hier könnte man auf den ersten Blick denken: Warum denn das schon wieder – es ist doch schon alles gesagt? Auf den zweiten Blick stellt sich die Sache ganz anders dar: Es wäre viel zu kurz gegriffen, wenn Datenschutz und IT-Sicherheit lediglich als lästige Pflichtaufgaben betrachtet werden. Das Thema lohnt sich – gerade jetzt!

Wir befinden uns auf der Zielgeraden des OZG und die Schwarze-Peter-Diskussion läuft bereits auf Hochtouren. Warum ist die Einführung der digitalen Verwaltung bis Ende dieses Jahres so krachend gescheitert? Gerne wird dann der überbordende Datenschutz in Deutschland als Sündenbock für gescheiterte Vorhaben und verzögerte Projekte ins Feld geführt.

Durch den Ukraine-Krieg ist das Thema Cyber-Security noch stärker in den Mittelpunkt von Verwaltungsführung und IT-Verantwortlichen gerückt. Das Bundesinnenministerium hatte hierzu im Sommer 2021 eine überarbeitete Cyber-Sicherheitsstrategie für Deutschland veröffentlicht. Ganz aktuell wurde kein Jahr später die Cyber-Sicherheitsagenda des BMI herausgegeben. Dort will man Schwachstellen durch die Zentralstellenfunktion des BSI mittels Änderung des Grundgesetzes beseitigen. Cyber-Kriminalität wird also jetzt durch eine neue Organisation der Sicherheitsarchitektur mit der führenden Rolle des Bundes bekämpft.

Diese beiden Beispiele verdeutlichen, dass auch auf der großen Bühne nach wie vor Diskussionsbedarf besteht. Das Narrativ vom Stolperstein „Datenschutz“ auf dem Weg in die digitale Verwaltung ist vorgeschoben. Und IT-Sicherheit ist kein notwendiges Übel, sondern unbedingte Voraussetzung dafür, dass die Digitalisierung gelingt!

Wir haben mit der DSGVO gute Leitplanken für den Datenschutz gesetzt, und auch der CERT-Verbund von BSI und Ländern hat sich in der Zusammenarbeit bei vielen Anlässen in der Praxis bewährt. Organisatorischer Aktionismus löst hier nicht unsere Probleme.

Mit unserem Kundenmagazin betrachten wir die Themen bewusst aus einer anderen Perspektive. Nämlich von unten: aus der Sicht der Umsetzenden vor Ort. Fakt ist: Wir brauchen Internetsicherheit und wir brauchen für Bürgerinnen und Bürger digitale Lösungen mit „gutem Datenschutz“, bei denen sie die Kontrolle und Transparenz – also die Hoheit – über ihre eigenen Daten behalten. Aber wir brauchen vor allen Dingen Lösungen!

Dabei sollten wir uns aber auf dem Weg in die moderne digitale Verwaltung immer wieder vor Augen führen: Die Nutzung digitalisierter Verwaltungsleistungen funktioniert nur dann komfortabel, wenn keine oder möglichst wenige der Daten manuell eingegeben werden müssen, die den Behörden sowieso bereits vorliegen. Hierfür brauchen wir zum Beispiel das integrierte Datenschutzcockpit.

Wir zeigen Ihnen in den Beiträgen dieser Ausgabe deshalb, was schon geht. Und nicht, warum etwas nicht funktioniert. Sie finden Fachbeiträge aus der Praxis und für die Praxis: Welche Konzepte es gibt, um IT-Sicherheit konkret vor Ort gegen ständig wachsende Bedrohungen zu verbessern, und wie man moderne Dienstleistungen digital und datenschutzkonform bereitstellt.

In diesem Sinne wünsche ich bei der Lektüre der Sommerausgabe wie immer viel Spaß und freue mich sehr über Anregungen und Ihr Feedback!

Ihr Bernd Landgraf
Geschäftsführer ITEBO-Unternehmensgruppe

Von unscheinbar bis unverzichtbar

ITEBO berät seit 16 Jahren zum Thema Datenschutz und IT-Sicherheit

Beratungsleistungen zu Datenschutz und IT-Sicherheit boomen. Das spürt auch die ITEBO-Unternehmensgruppe. Was heute ein eigener Servicebereich mit einer dreistelligen Kundenzahl ist, wurde früher nebenbei betreut. Nach 16 Jahren haben die Datenschutz- sowie IT-Sicherheitsexpertinnen und -experten viel gemeinsam erlebt und geleistet. Dank ihnen ist die ITEBO-Unternehmensgruppe ein kompetenter und leistungsstarker Ansprechpartner für alle Themen um Informationssicherheit und Datenschutz.

Schrittweises Wachstum

2006 dachten viele Kommunen noch nicht an Datenschutz. Eine Ausnahme war der erste Kunde im Datenschutzbereich der ITEBO: die Gemeinde Bohmte. Schon damals deutete es sich an, dass dieses Thema zukünftig überaus wichtig werden würde. Bernhard Hehmann, heute bekannt als Servicebereichsleiter des Outputmanagements, war damals im UserHelpDesk (heute ServiceDesk) angestellt und zunächst „nur“ interner Datenschutzbeauftragter (DSB). Aus seiner Funktion als interner DSB entwickelte er geeignete Ideen, um den Kundinnen und Kunden der ITEBO die Beratung und Unterstützung zum Datenschutz als Service „externer Datenschutzbeauftragter“ anzubieten. Es folgten weitere Mitarbeiter, unter ihnen Kim Schoen. Er berät Kunden seit 2014 als externer Datenschutzbeauftragter.

Die Anzahl der Kunden wuchs genauso wie die Mitarbeiterzahl. Schon bald wurde ein eigenständiges Team notwendig. Rund elf Jahre nach dem ersten Kunden wurde Datenschutz ein eigener Servicebereich im Geschäftsbereich Anwendungen. Schon bald erlangte dieses Feld noch mehr Aufmerksamkeit, denn die DSGVO sowie weitere geänderte Datenschutzgesetze kündigten sich an. Die DSGVO trat 2016 mit einer zweijährigen Übergangszeit in Kraft und bedeutete für viele Einrichtungen zahlreiche Veränderungen und auch eine Menge Arbeit. Dies galt umso mehr, weil zusätzlich viele deutsche Fachgesetze und Verordnungen an die Datenschutzgesetzgebung angepasst werden mussten. Teilweise wurden Gesetze auch erst nach der Übergangszeit angepasst. So wurden am 26.11.2019, 18 Monate nach Inkrafttreten der DSGVO, mit dem 2. Da-

tenschutz-Anpassungs- und -Umsetzungsgesetz des Bundes (DSAnpUG) 155 weitere Gesetze an die neue Datenschutzgesetzgebung angepasst.

Für die meisten Unternehmen und Verwaltungen bedeutete dies nicht nur einen erhöhten Beratungsbedarf, sondern auch einen hohen Umsetzungsdruck. In dieser Zeit stieg die Anzahl der Kundinnen und Kunden im Datenschutzbereich noch einmal deutlich. Zum Glück hatte die ITEBO-Unternehmensgruppe den Bereich bereits im August 2019 nochmals neu strukturiert. Weil das Thema Informationssicherheit als weiterer Schwerpunkt neben der Datenschutzberatung immer stärker nachgefragt wurde, war diese Neuordnung nötig.

Vielseitiges Aufgabenfeld durch verschiedenste Kunden

Heute sind die Anforderungen und Aufgaben, die im Servicebereich auf die Mitarbeiterinnen und Mitarbeiter warten, so vielfältig wie nie. Das liegt zum einen an der Größe der Unternehmen, öffentlichen Stellen und kirchlichen Einrichtungen, zum anderen jedoch auch an der Vielfalt der Branchen und daraus resultierender individueller Besonderheiten. Denn, neben der bekannten DSGVO, die EU-weit gilt, gibt es in Deutschland ergänzend das Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze der Bundesländer (NDS=NDSG), Datenschutzgesetze der Evangelischen Kirche Deutschland (DSG-EKD) und der Katholischen Kirche (KDG).

So betreut der Servicebereich kleine und mittelständische Unternehmen und Kommunen genauso wie auch das Erzbistum Hamburg. Dieses stellt mit dem KDG (Gesetz über den Kirchlichen Datenschutz) und Einrichtungen von Schulen bis hin zu Beratungsstellen noch einmal neue Anforderungen an die Expertinnen und Experten der ITEBO. Eine Herausforderung, welche die zertifizierten Datenschützerinnen und Datenschützer jedoch sehr gerne annehmen und meistern.

Weiter auf der folgenden Seite »

Besondere Herausforderungen begegnen dem Team immer wieder auch durch die Überraschungen, die die Informationssicherheit bereithält. So waren die ersten Beratungsthemen, mit der die ITEBO-Unternehmensgruppe ihre Kunden unterstützte, die im Jahre 2018 bekannt gewordenen Sicherheitslücken in den Intel CPU-Prozessoren „Meltdown“ und „Spectre“.

Die Expertise externer Datenschutzbeauftragter bewährt sich in der Praxis. Laut einer Veröffentlichung des Landesrechnungshofes in Niedersachsen aus dem Jahr 2017 haben Kommunen mit externen Datenschutzbeauftragten deutlich weniger offene Handlungsbedarfe als Kommunen mit internen Datenschutzbeauftragten. Das wirkt sich auch auf die Kosten aus.

Kim Schoen kennt die Gründe dafür: „Auftragsverarbeitung, Datenschutzbewertung und Datenschutz-Folgenabschätzung: Für uns ist das Tagesgeschäft. Daher arbeiten wir in der Regel effizienter und zielgerichteter als Mitarbeiter, für die der Datenschutz nur eine zusätzliche Aufgabe ist. Das hat ein Prüfbericht nun auch bestätigt.“

Weitere wichtige Faktoren dürften der ständige Austausch mit den Kunden wie auch die zahlreichen Schulungen sein, die das Team dieses Servicebereichs absolviert, um stets auf dem aktuellen Stand zu sein. Aus diesem Grund ist die ITEBO-Unternehmensgruppe auch Mitglied in der Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD).

Nicht nur Unternehmen, Verwaltungen und kirchliche Einrichtungen profitieren von der Expertise der ITEBO-Unternehmensgruppe. Ganz aktuell hat Majid Cirousse, den Sie als Servicebereichsleiter vielleicht bereits kennen, einen Lehrauftrag erhalten. Er darf an der Hochschule Osnabrück Studierende des Studiengangs Öffentliche Verwaltung zum Thema Datenschutzrecht und IT-Recht unterrichten.

Ihr Team für Datenschutz und IT-Sicherheit

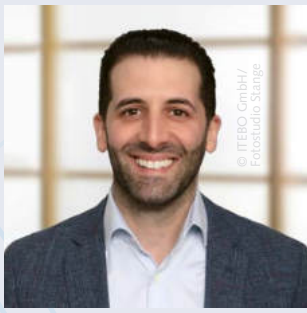
Das Datenschutz- und IT-Sicherheits-Team der ITEBO besteht nicht nur aus Juristen, sondern ebenfalls aus Spezialisten der verschiedensten Bereiche. Die daraus resultierende Vielseitigkeit und Ganzheitlichkeit weiß auch Majid Cirousse besonders zu schätzen: „Als ich 2020 bei der ITEBO anfing, konnte ich direkt mit einem hochspezialisierten Team starten. Das hat von Anfang an sehr gut funktioniert. Alle Kolleginnen und Kollegen haben ihre Spezialgebiete, sodass wir gut für die unterschiedlichen Anforderungen unserer Kunden aufgestellt sind. Die Vielfältigkeit unserer Ausbildungen und Expertisen zählt für mich zu unseren besonderen Stärken, weil wir dadurch ganzheitlich beraten können.“

Alexander Fischer ist seit 2017 Datenschutz- und Informationssicherheitsberater sowie externer Datenschutzbeauftragter bei der ITEBO-Unternehmensgruppe. Alexander Fischer ist ein Allround-Talent, das KMUs, Verbände und Vereine wie auch Stiftungen und Behörden berät. Er zeichnet sich auch durch seine Expertise bei der Etablierung von Regelwerken, Erstellung des Verzeichnisses von Verarbeitungstätigkeiten und Durchführung von Bestandsaufnahmen aus. Als Wirtschaftsinformatiker und IT-Grundschutz-Praktiker ist die Schnittmenge zwischen dem Datenschutz und der Informationssicherheit seine Passion. Zudem führt er Schulungen durch und lässt so andere auch von seinem Wissen profitieren.

Seit 2020 ist der studierte Wirtschaftsjurist **Eric-Josua Themann** bei der ITEBO-Unternehmensgruppe als Informationssicherheits- und Datenschutzberater tätig. Sein Spezialgebiet ist der Datenschutz in kirchlichen Einrichtungen. Er ist zudem der richtige Ansprechpartner beim datenschutzrechtlichen Umgang mit Fotografien, der Durchführung von Datenschutz-Folgenabschätzungen und der Formulierung von Auftragsverarbeitungsverträgen, Datenschutzerklärungen und der Durchführung von Bestandsaufnahmen.

Kim Schoen war der dritte Mitarbeiter der ITEBO, der sich auf den Datenschutz spezialisiert hat und verfügt über herausragendes Wissen und vielfältige Erfahrungen im Bereich der Informationssicherheit. Er ist außerdem Datenschutzbeauftragter der ITEBO-Unternehmensgruppe und TÜV-geprüfter IT-Security-Beauftragter/Manager und auf kommunale Einrichtungen, Krankenhäuser, Schulen, Wasser- und Bodenverbände sowie Wirtschaftsunternehmen spezialisiert. Zu seinen Beratungsschwerpunkten gehören unter anderem datenschutzrechtliche Aspekte der Videoüberwachung und die Vor-Ort-Kontrolle von Dienstleistern. Zudem unterstützt er ITEBO-Kunden bei der Etablierung von Managementsystemen für Datenschutz und Informationssicherheit und unterstützt diese darüber hinaus bei eigenen Audits oder Prüfungen von Aufsichtsbehörden.

Bereits seit 2011 beschäftigt sich **Klaus Exner** beruflich intensiv mit dem Datenschutz; bei der ITEBO-Unternehmensgruppe ist er seit 2018 angestellt. Der Informationssicherheits- und Datenschutzbeauftragte hat sich auf öffentliche Einrichtungen, Baudienstleister, Stiftungen, kirchliche Einrichtungen wie auch Unternehmen der freien Wirtschaft spezialisiert. Er berät unter anderem bei der Planung und Einführung von Videoüberwachungsanlagen sowie speziell zu Beschäftigten- und Kundendatenschutz oder Datenschutz-Folgenabschätzungen.. Außerdem ist er beratend bei der Etablierung von ISMS und DSMS tätig.



Majid Cirousse ist seit September 2020 bei der ITEBO als Servicebereichsleiter des Servicebereichs Datenschutz und IT-Sicherheit tätig. Der gelernte Jurist und Banker kann auf eine langjährige Erfahrung im Bereich des Datenschutzrechts zurückblicken. Unter anderem war er im Niedersächsischen Datenschutzzentrum tätig. Wissen weiterzugeben, liegt Majid Cirousse am Herzen. Deutlich wird dies durch seinen Lehrauftrag an der Hochschule Osnabrück genauso wie durch seine Trainertätigkeit im Nachwuchsleistungszentrum des VfL Osnabrück.

Als Werkstudentin ist **Angélique Schwarz** seit Dezember 2020 im Servicebereich Datenschutz und IT-Sicherheit tätig. Sie hat ihren Bachelor of Laws im April 2022 erfolgreich abgeschlossen und strebt nun einen Masterabschluss in Wirtschaftsrecht im Sommer 2023 an. Ihre Schwerpunkte sind Datenschutz und das Recht des geistigen Eigentums und der Digitalisierung.

Ganz neu im Team ist **Laura Kleine-Tebbe**, die seit August 2022 als Datenschutzberaterin bei der ITEBO tätig ist. Nach einem Bachelor in Wirtschaftsrecht (LL.B) an der Fachhochschule Bielefeld im März 2021 hat sie ihr Masterstudium in Wirtschaftsrecht (LL.M) im Juli 2022 an der Hochschule Osnabrück absolviert. Ihre Schwerpunkte sind neben Datenschutz auch das Recht der Digitalisierung sowie Vertrieb- und Handelsrecht.

Datenschutz und IT-Sicherheit

Ähnlich, aber doch ganz anders

Wir leben in einer Informationsgesellschaft, deren Rohstoff Daten sind. Doch was ist, wenn ein Mensch nicht möchte, dass persönliche Informationen anderen als Grundlage ihres Handelns dienen? Wenn er sich dagegen sträubt, dass ein Online-Shop ein Nutzerprofil über ihn erstellt, sein EKG auf US-Servern lagert oder seine Suchmaschine seine geheimsten Fragen auch dann kennt, wenn er nur nach neuen Schuhen sucht?

Daten bestimmen heute mehr denn je über Geld und Macht. Wer seine Kunden besser kennt, kann mehr an sie verkaufen. Wer die Sorgen und Bedürfnisse der Bevölkerung kennt, überzeugt mehr Wähler. Daten sind so wertvoll wie nie zuvor.

Deswegen liegt es in der Verantwortung von Kommunen, kirchlichen Einrichtungen und Unternehmen, die persönlichen Daten zu schützen und sorgsam mit ihnen umzugehen. Doch nicht jedem, der mit Daten zu tun hat, sind die Zuständigkeiten und Begrifflichkeiten klar. Nicht nur die persönlichen Daten müssen geschützt werden. Datenschutz und Datensicherheit sind zwei völlig unterschiedliche Begriffe mit verschiedenen Ausprägungen. Die ITEBO-Unternehmensgruppe verfügt über Expertise für beides und unterstützt Kommunen sowie Unternehmen schon seit vielen Jahren dabei, dies entsprechend zu gewährleisten.

Das Recht auf informationelle Selbstbestimmung als Grundlage des Datenschutzes

Welche Wichtigkeit Daten haben, rückt immer stärker in das Bewusstsein von Einzelpersonen. Doch schon vor vierzig Jahren, also noch weit vor der Verbreitung des Internets, wurde dieses Thema politisch kontrovers behandelt. Debatten um den damaligen Zensus führten schließlich dazu, dass der Bundesgerichtshof 1983 sein sogenanntes Volkszählungsurteil erließ.

Dieses sollte verhindern, dass gesammelte Daten zu einem Persönlichkeitsprofil zusammenfließen könnten. Die Bedenken damals richteten sich jedoch vor allem auf Einschüchterungseffekte bei abweichendem Verhalten. Um zu verhindern, dass die eigenen Daten gegen Menschen verwendet werden können, etablierte das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung und gliederte es an das allgemeine Persönlichkeitsrecht an. Noch heute gilt es als die wichtigste Grundlage für den Datenschutz. Durch dieses Gesetz benötigt selbst der Staat eine rechtliche Grundlage, um Daten erheben und verarbeiten zu dürfen.

Verantwortliche dürfen Daten nur in einem Ausmaß und auf eine Weise verarbeiten, für die sie eine Rechtsgrundlage haben. Verstoßen sie gegen die geltenden datenschutzrechtlichen Gesetze, verhängen Aufsichtsbehörden unter Umständen Bußgelder. Alle rechtlichen Vorgaben, die das Recht der Person auf informationelle Selbstbestimmung absichern sollen, fallen unter den Datenschutz. Dieser hat sich in den letzten Jahrzehnten auch durch die neuen Anforderungen des Internets noch einmal deutlich weiterentwickelt. Außerdem wurde er auf EU-Ebene harmonisiert.

Weiter auf der folgenden Seite »

Datenverarbeitende Instanzen in der Pflicht: Rechte schützen und Daten sichern

Für Unternehmen und Kommunen bedeuten die Maßgaben des Datenschutzes auch, dass sie sich mit der Sicherheit der Daten auseinandersetzen müssen. Doch Datenschutz beinhaltet dabei nicht den Schutz der Daten, sondern vielmehr den Schutz der Rechte natürlicher Personen. Den Schutz aller Daten bezeichnen hingegen viele IT-Expertinnen und -Experten als „Datensicherheit".

Die ITEBO-Unternehmensgruppe spricht in diesen Fällen allerdings seltener von der Datensicherheit, sondern lieber von der Informationssicherheit. Denn diese umfasst sämtliche Informationen eines Unternehmens, einer kirchlichen Einrichtung oder einer Verwaltung und nicht nur Daten. Dieser Begriff ist durchaus eng mit dem Datenschutz verknüpft.

Schließlich ist die Informationssicherheit aufgrund des Datenschutzes unabdingbar: Wer Daten von Personen erhebt, muss dafür Sorge tragen, dass sie nicht in die Hände von Unbefugten gelangen. Bei der Informationssicherheit geht es jedoch nicht exklusiv um den Datenschutz. Stattdessen möchten Unternehmen oder Kommunen die Sicherheit ihrer Daten und Informationen erreichen.

Diese müssen nicht auf Personen bezogen sein, sondern können beispielsweise auch Forschungsdaten, betriebswirtschaftliche Informationen oder andere Erkenntnisse enthalten. Solche Informationen sollte ein Unternehmen jedoch genauso vor dem unberechtigten Zugriff Dritter schützen wie die Daten einer Person. Datensicherheit könnte also ohne Datenschutz existieren, Datenschutz jedoch nicht ohne Datensicherheit.

Schutzziele der Informationssicherheit: tägliches Brot der ITEBO

Die Informationssicherheit hat verschiedene Schutzziele, mit denen sie den Datenschutz sicherstellen soll. Das erste Ziel ist die **Vertraulichkeit**. Diese kann die ITEBO-Unternehmensgruppe beispielsweise umsetzen, indem sie strikte Rollen für einzelne Mitarbeiter vergibt. Viele der von uns eingesetzten Lösungen nutzen sehr dezidierte Zugangsberechtigungen und sichern die Vertraulichkeit so für alle Daten und Personen. Auf diese Weise verhindern Kommunen, kirchliche Einrichtungen und Unternehmen einen unbefugten Zugriff auf Daten: Sachbearbeiterinnen und Sachbearbeiter können dadurch nur die Daten bearbeiten und lesen, die für ihre Arbeit relevant sind.

Ein weiteres Schutzziel ist die **Integrität**. Sie ist nur gegeben, wenn alle Daten und Systeme korrekt und unverändert funktionieren. Die Integrität geht hingegen verloren, wenn Systeme nicht korrekt arbeiten oder Daten verfälscht werden. Eine Möglichkeit, diese Integrität sicherzustellen, sind deswegen die zahlreichen Fehleranalysen und Testläufe, welche die ITEBO-Mitarbeiterinnen und -Mitarbeiter durchführen, um sicherzugehen, dass Hard- und Software funktionieren. Außerdem ist auch die Verschlüsselung ein unabdingbares Hilfsmittel hierfür, welches die ITEBO-Expertinnen und -Experten täglich einsetzen.

Bei der **Authentizität** handelt es sich um ein weiteres Schutzziel im Rahmen der Informationssicherheit. Diese ist dann gefährdet, wenn Unbefugte Daten versenden. Für kommunale und städtische Verwaltungen hat dieses Thema natürlich eine besondere Wichtigkeit, denn die Dokumente, die sie ausstellen, müssen stets höchsten Ansprüchen an Authentizität genügen. Deswegen ist es für sie auch von besonderer Bedeutung, dass Mitteilungen an und von Bürgerinnen und Bürgern absolut echt, zuverlässig und glaubwürdig sind sowie vom berechtigen Absender stammen. Die ITEBO-Unternehmensgruppe bietet Verwaltungen deswegen diverse Möglichkeiten, mit denen sich Bürgerinnen und Bürger, aber auch Kommunen, beim Versenden von Daten authentifizieren können. Die Möglichkeiten beginnen bei qualifizierten elektronischen Signaturen und reichen bis hin zu sicheren Bürgerprofilen im OpenR@thaus.

Das vierte Schutzziel ist die **Verfügbarkeit**. Daten und Systeme müssen jederzeit von autorisierten Personen genutzt werden können. Dieses Schutzziel ist nicht zuletzt eine der Kernkompetenzen der ITEBO-Rechenzentren. Hier stellen Mitarbeiterinnen und Mitarbeiter Tag und Nacht sicher, dass Server online sind und die Systeme der Kundinnen und Kunden funktionieren.

Datenschutz und Informationssicherheit haben nicht immer das gleiche Ziel

Datenschutz, Datensicherheit und Informationssicherheit: Diese Begrifflichkeiten auseinanderzuhalten, ist nicht immer leicht. Dabei kann es sogar vorkommen, dass sich Datenschutz und Informationssicherheit widersprechen. Will beispielsweise ein Unternehmen den Zeitpunkt und die Dauer tracken, wann eine Mitarbeiterin oder ein Mitarbeiter sich in ein System eingeloggt hat, dient dies der Datensicherheit. Schließlich lassen sich durch dieses Tracking Schutzziele wie Integrität und Vertraulichkeit besser sicherstellen. Datenschützer könnten dies hingegen kritisch sehen, weil das Speichern dieser Daten durchaus Persönlichkeitsrechte berührt.

Deswegen ist es oft nicht förderlich, Datenschutz und Informationssicherheit strikt zu trennen. Im Gegenteil sind es nicht zuletzt die Unterschiede, das Spannungsfeld und die Überschneidungen zwischen diesen beiden Begriffen, durch welche die wichtigsten Entscheidungen getroffen werden. Gemeinsam mit den Kunden arbeitet die ITEBO-Unternehmensgruppe daran, Lösungen zu finden, die sowohl den Anforderungen der Informationssicherheit als auch denen des Datenschutzes genügen. Die ITEBO-Mitarbeitenden unterstützen sie dabei, Spannungen zwischen diesen Anforderungen zu lösen und Synergien zu nutzen.

ITEBO data skydd

Keine Angst vor der Informationspflicht

ITEBO dataskydd unterstützt Datenschutzmanagement

Wer seine Rechte nicht kennt, kann sie nicht wahrnehmen. Auf die Datenverarbeitung bezogen bedeutet das: Nur wer weiß, wo welche seiner Daten verarbeitet werden, kann auch die Betroffenenrechte wahrnehmen. Darunter fallen beispielsweise das Recht auf Auskunft, das Recht auf Löschung wie auch das Recht der Einschränkung der Verarbeitung. Deswegen müssen datenschutzrechtliche Verantwortliche alle Personen, von denen Daten verarbeitet werden, über diese Verarbeitung informieren. So wollen es die Datenschutzgesetze. Die Informationspflicht ist eine mehr oder weniger direkte Folge des Grundrechts auf informationelle Selbstbestimmung und sollte nicht nur wegen der empfindlichen Strafen bei Verstößen ernstgenommen werden.

Informationspflicht in Kommunen, kirchlichen Einrichtungen und Unternehmen

Das sorgt bei datenschutzrechtlich Verantwortlichen auch heute noch für viele Unsicherheiten. Kaum ein Thema sorgt für so viele Nachfragen wie die Erfüllung von Informationspflichten, weiß auch Eric-Josua Themann, Informationssicherheits- und Datenschutzberater bei der ITEBO-Unternehmensgruppe:

„Die Erfüllung von Informationspflichten ist ein regelmäßiges Thema bei vielen unserer eDSB-Kunden. Insbesondere bei der Einführung komplexerer Verarbeitungen personenbezogener Daten bestehen teilweise Unsicherheiten zu den Fragen: „Wer muss informiert werden?“, „Wann muss die Information zur Verfügung gestellt werden?“, „Worüber muss konkret informiert werden?“ oder „Auf welche Art und Weise kann die Information erfolgen?“ Bei der Beantwortung dieser Fragen unterstützen wir unsere Kunden gerne mit Rat und Tat.“

Denn in der Praxis sind die Informationspflichten durchaus komplex, zumal zwischen Direkterhebung und Dritterhebung unterschieden werden muss. Bei der Direkterhebung erhalten datenschutzrechtlich Verantwortliche die Daten direkt von der betroffenen Person. Aber auch, wer Daten aus anderen Quellen erhält, hat regelmäßig Informationspflichten zu beachten. Es handelt sich dann um eine sogenannte Dritterhebung.

Personen haben umfangreiche Auskunftsrechte

Menschen, deren Daten verarbeitet werden, haben in der EU nicht nur das Recht darauf, dies zu erfahren. Sie müssen auf Nachfrage zudem im Detail darüber informiert werden, welche Daten wo und wie über sie gespeichert und verarbeitet werden. Aus den Datenschutzgesetzen ergibt sich, dass Kommunen, kirchliche Einrichtungen und Unternehmen zahlreiche Informationen zur Verfügung stellen müssen. Um welche Daten es sich konkret handelt, ist in Teilen Auslegungssache.

Klar ist jedoch, dass Betroffene umfangreich darüber informiert werden müssen, wer die Daten verarbeitet. Darunter fallen Verantwortliche und Datenschutzbeauftragte mit Namen und Kontaktdaten. Auch Teile der Verarbeitung sind offenzulegen. Betroffen sind hier beispielsweise die automatisierte Entscheidungsfindung oder das Profiling, die Kategorie der Daten, ihre Quellen und ihre Empfänger. Personen müssen zudem über Zweck und Rechtsgrundlage der Datenerhebung informiert werden.

Weiter auf der folgenden Seite »

Layered approach praxistauglicher

Wer Kontakte direkt mit allen verfügbaren Informationen versorgt, erzielt dadurch nicht immer maximale Transparenz. Denn zu umfangreiche Datenschutzerklärungen führen oft dazu, dass Betroffenenrechte darin untergehen. Wer praxisnah informieren möchte, verfährt deswegen häufig nach einem Schichtprinzip. Dabei erhält der Betroffene nicht direkt alle Informationen, sondern wird im ersten Schritt mit den notwendigsten versorgt.

Bezogen auf das Beispiel einer Website wäre die erste Informationsschicht der Cookie-Banner mit dem Hinweis, dass die Website Cookies setzt und diese verwertet. Klicken Userinnen und User auf entsprechende Formulierungen, können sie genau auswählen, welche Zwecke und welche Unternehmen ihre Daten nutzen dürfen. Sie erhalten auf Nachfrage mehr Transparenz durch die zweite Informationsschicht. Für noch Neugierigere steht die Datenschutzerklärung bereit, in der alle rechtlichen Grundlagen haarklein ausformuliert sind. Wer es genau wissen will, hat außerdem noch die Möglichkeit, bei den Verantwortlichen eine Auskunft über die von ihm gespeicherten Daten zu beantragen.

Ein ähnliches Prinzip ist auch mit Medienbrüchen möglich: Ein Hinweisschild zeigt an, dass der Betroffene gefilmt wird. Per QR-Code kann er sich genauere Informationen zur Datenverarbeitung aus dem Internet ziehen. Informationen im ersten Schritt zurückzuhalten, stärkt die Transparenz also sogar. Man stelle sich vor, jeder Konzertbesucher würde eine Akte mit Dutzenden Seiten Datenschutzerklärung erhalten. Der Nutzen wäre gering und die Rechte würden in juristischen Notwendigkeiten untergehen.

Doch dieses auch als „layered approach“ bezeichnete Prinzip ist nicht in allen Fällen sinnvoll. Die ITEBO-Unternehmensgruppe berät Sie gerne bei der Auswahl der besten Herangehensweise.

Wer muss wann informieren?

Wer personenbezogene Daten erhebt, muss die Betroffenen darüber informieren. Diese Informationspflicht gilt übrigens nicht nur für Bürgerinnen und Bürger oder Kundinnen und Kunden, sondern auch für Angestellte oder Geschäftspartnerinnen und Geschäftspartner.

Die einfachste Antwort auf die Frage, wann ein Betroffener informiert werden muss, ist: Grundsätzlich immer, wenn personenbezogene Daten erhoben werden und sofort im Moment der Datenerhebung. Es gibt zwar einige Ausnahmen, allerdings sind die durchschnittlichen ITEBO-Kunden davon üblicherweise nicht betroffen. Stammen die Daten von Dritten, müssen Betroffene innerhalb eines Monats informiert werden. Dies gilt allerdings nicht, wenn die betroffene Person schon informiert worden ist. Dann ist die Informationspflicht bereits erfüllt.

Verwaltungen sind besonders in der Pflicht

Für Verwaltungen ist die Lage noch einmal komplizierter. Dies hat diverse Gründe. Einerseits werden relativ viele und zudem sehr sensible Daten erfasst. Des Weiteren erhöht sich durch die zunehmende Digitalisierung der Prozesse die Komplexität der eingesetzten Systeme.

Beispielsweise ist die ITEBO-Unternehmensgruppe wie jeder andere IT-Dienstleister auch ein weiterer Faktor. Denn auch sie speichert Daten und stellt diese der Kommune wieder zur Verfügung. Seien es die Portallösungen wie OpenR@thaus oder andere Fachverfahren, die auf den Cloud-Servern laufen: Auch das müssen Kommunen bei ihren Informationspflichten beachten.

Das Problem: Eine Datenschutzerklärung für alle Prozesse reicht rechtlich nicht aus. Denn alle Angaben müssen einen eindeutigen Bezug haben und die Prozesse widerspiegeln. Dies bedeutet, dass Datenschutzerklärungen konkret ausformuliert werden müssen. Mithilfe von Textbausteinen lässt sich dieses Problem jedoch relativ leicht lösen.

ITEBO dataskydd für effizienteres und übersichtlicheres Datenschutzmanagement

„Bei der ITEBO setzen wir auf dataskydd, um das Datenschutzmanagement einfach und effizient zu organisieren. Die Plattform unterstützt unsere Kundinnen und Kunden bei allen Aufgaben rund um den Datenschutz. Mit der Einführung der neuen Datenschutzmanagementsoftware ITEBO dataskydd möchten wir unseren Kunden eine ganzheitliche Lösung zur Etablierung einer Datenschutzorganisation anbieten. Alle Anforderungen der Datenschutzgesetzgebung könnten somit auf der Plattform abgebildet werden“, ist Informationssicherheits- und Datenschutzberater Alexander Fischer von der IT-Lösung überzeugt.

ITEBO dataskydd

Wie die meisten IT-Lösungen, die die ITEBO-Unternehmensgruppe anbietet, ist auch dataskydd modular aufgebaut. Eines der wichtigsten Module ermöglicht ITEBO-Kundinnen und -Kunden, Vereinbarungen zur Auftragsverarbeitung (AVV) zu erstellen und zu verwalten. Im gleichen Zuge kann jede AVV mit einem Status versehen und einer Verarbeitungstätigkeit zugeordnet werden. Über die Workflowfunktion können die beteiligten Fachabteilungen an der Erstellung der Vereinbarungen zur Auftragsverarbeitung mitwirken. Teil des Moduls ist auch das Vertragsmanagement, das die Prüfung von AV-Vereinbarungen durch den DSB ermöglicht.

Ein reibungsloser Workflow ist das Kernstück der Software. Sie deckt verschiedene Funktionen und Bedarfe ab: Egal ob es darum geht, dass alle beteiligten Fachabteilungen Aufgaben verwalten, Maßnahmen zur Verhinderung von Verstößen geplant oder Datenschutzverletzungen gemeldet werden müssen, dataskydd ermöglicht eine gezielte Kontrolle, weil es eine praxistaugliche Aufgabenverwaltung und den übersichtlichen Maßnahmenplan nutzt. Möglich wird dies auch durch klare Verantwortlichkeiten: Jede Aufgabe verfügt über Verantwortliche, Zieldatum und Status. Auf diese Weise können alle Beteiligten ihre Aufgaben überblicken und wissen, bis wann diese fällig sind.

Weiter auf der folgenden Seite »

VVT mit dataskydd deutlich einfacher und rechtssicher

Eine weitere Spezialität von ITEBO dataskydd ist das Verzeichnis der Verarbeitungstätigkeiten (VVT). Das Führen eines solchen ist für beinahe alle datenschutzrechtlich Verantwortlichen Pflicht. Es handelt sich dabei um eine Auflistung aller Prozesse, in denen personenbezogene Daten verarbeitet werden. Ziel ist es, eine Übersicht über die Datenverarbeitungen zu erlangen.

Um dieses Ziel zu erreichen, müssen alle personenbezogenen Daten ermittelt werden, die Verwaltungen, Kirchen und Unternehmen verarbeiten. Dafür müssen Verantwortliche alle Tools, Software-Produkte sowie Prozesse eruieren. Gerade dann, wenn fortgeschrittene Digitalisierung, viele Tools sowie eine vielseitige Datennutzung zusammenkommen, sind durchaus mehr als 100 Einträge erforderlich.

Schnelles, transparentes und effizientes Erfüllen von Informationspflichten

Obwohl das VVT auch zu Dokumentationszwecken erstellt wird, hat es einen entscheidenden Vorteil: Datenschutzrechtlich Verantwortliche wissen, wo welche Verarbeitungen dieser Daten erfolgen. Dadurch können sie sowohl den Betroffenen als auch den Aufsichtsbehörden schnell und zeitnah Auskünfte erteilen. Dafür muss das VVT allerdings einen hohen Reifegrad aufweisen können.

Mithilfe eines Leitpfades werden Nutzerinnen und Nutzer bei der Erstellung des VVT begleitet. Das Programm ermöglicht allen verantwortlichen Fachabteilungen, das VVT separat zu bearbeiten und so aktuell zu halten. Eine weitere Stärke des Programms: Durch die Exportfunktion kann die Rechenschafts- sowie Informationspflicht jederzeit erfüllt werden. Dies gilt sowohl gegenüber Betroffenen als auch gegenüber den zuständigen Aufsichtsbehörden. Das ist wichtig, denn die Zeit drängt: Beispielsweise haben betroffene Personen ein Auskunftsrecht, das innerhalb von einem Monat erfüllt werden muss.

Datenschutzrechtlich Verantwortliche wie die Samtgemeinde Rethem profitieren von dem Wissen erfahrener Datenschutzbeauftragter, weiß auch Petra Schulze: „Wir sind froh, dass uns die ITEBO bei der Erstellung des VVT so gut und umfassend unterstützt hat. Ganz allein wäre es schwierig geworden. Auch die technische Umsetzung im Programm dataskydd ist klar und übersichtlich gestaltet. Wir freuen uns, dass wir diesen Baustein bei der Erfüllung der Vorgaben der DSGVO erfolgreich umsetzen konnten. Es werden bestimmt noch weitere Projekte folgen.“

dataskydd legt großen Wert auf die Arbeitserleichterung. Deswegen sind viele standardisierte Inhalte bereits vorgegeben. Darunter fallen beispielsweise die Kategorien von personenbezogenen Daten, Kategorien von betroffenen Personen sowie technische und organisatorische Maßnahmen. Individuelle Textbausteine erleichtern und beschleunigen die Arbeit.

Alexander Fischer führt aus: „Mithilfe von Eingabeformularen sowie vielfältigen Verknüpfungen in der Datenbank lässt sich das VVT (zeit-)effizient erstellen. Aus zahlreichen Projekten bekommen wir diesbezüglich positive Rückmeldungen. Weitere Synergieeffekte können bei der Erstellung von Datenschutzhinweisen erzielt werden: Sobald eine Verarbeitungstätigkeit erfasst ist, lassen sich Datenschutzhinweise im Word-Format automatisiert generieren."

VVT hilft, Risiken zu steuern und zu kontrollieren

Das VVT dient dabei auch als Grundlage für weitere Funktionen von ITEBO dataskydd. So wird auf dieser Basis auch eine Datenschutz-Folgenabschätzung möglich. Diese ist dann erforderlich, wenn eine Datenverarbeitung sensibler personenbezogener Daten im großen Umfang erfolgen soll oder ein Einsatz von neuen Technologien geplant ist. dataskydd bietet Verantwortlichen eine standardisierte Risikobewertungsmatrix. Je sensibler die Daten, umso höher ist das Risikoniveau. Eine Dokumentation dieser Bewertung ist dann unumgänglich, außerdem dient diese als Grundlage für passende Schutzmaßnahmen.

Und auch bei der Dokumentation der technischen wie auch organisatorischen Maßnahmen unterstützt das Datenschutzmanagement-Tool. Nutzerinnen und Nutzer können Maßnahmenkataloge anlegen, welche daraufhin mit den jeweiligen Verarbeitungstätigkeiten verknüpft werden.

Wenn Datenschutzvorfälle trotzt der Sicherheitsmaßnahmen nicht verhindert werden können, unterstützt ITEBO dataskydd datenschutzrechtlich Verantwortliche, diese zu dokumentieren. Im Modul „Datenschutz- und Sicherheitsvorfälle" werden Verstöße hinsichtlich der gesetzlichen Meldepflicht geprüft und dokumentiert, was eine lückenlose Dokumentation der Ereignisse ermöglicht. Alle notwendigen Daten werden erfasst, sodass der Verantwortliche den Vorfall ggf. direkt an die Aufsichtsbehörde melden kann.

Onlineschulungsplattform

Alle, die sich mit IT-Sicherheit beschäftigen, wissen: Eine Software ist immer nur so gut und sicher, wie Anwenderinnen und Anwender erlauben. Damit Mitarbeitende auf dem aktuellen Stand bleiben, stellt die ITEBO mit der E-Learning-Plattform **ITEBO Lära** unterschiedliche Schulungen zur Verfügung. Die Onlinekurse wie z. B. „Datenschutz in der Kommunalverwaltung" bieten somit ein ergänzendes Angebot zu den Präsenzschulungen vor Ort. Ein Abschlusstest sichert nicht nur, dass Teilnehmerinnen und Teilnehmer die Lerninhalte verstanden haben. Er dient darüber hinaus der Dokumentation der Schulungsmaßnahme für den Personalbereich.

Wenn das Unwahrscheinliche eintritt

Schäden begrenzen mit effizientem Notfallmanagement

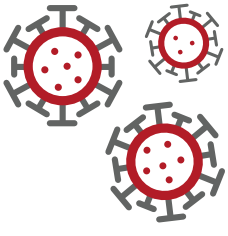
Wer sich nur darauf berief, dass unwahrscheinliche Ereignisse nicht eintreffen werden, ist spätestens seit der Corona-Pandemie geläutert. Stromausfälle, Cyberangriffe, Hochwasser oder schlichte Fehlkonfiguration: Was zunächst unwahrscheinlich wirkt, kann dennoch eine reale Gefahr darstellen.

Das weiß auch der Landesrechnungshof Niedersachsens. Dieser führt neben der externen Finanzkontrolle der kommunalen Körperschaften aktuell Schwerpunkt-Prüfungen zur Informationssicherheit mit dem Vertiefungsthema „Notfallmanagement“ durch. Auch der Bund macht zunehmend konkrete Vorgaben zur Informationssicherheit bei ebenenübergreifend Verfahren.

Sehen wir uns jedoch zuerst einige der „unwahrscheinlichen“ Ereignisse an:

Beispiel 1: Corona

Eine Pandemie mit einem hochansteckenden Virus, der Menschen töten kann: Dass ein solcher Fall möglicherweise auftreten könnte, war bekannt. Dennoch handelte es sich beim Corona-Virus um das, was in IT-Kreisen als „Zero-Day-Exploit“ gefürchtet ist. Ohne größere Vorwarnzeit bei gleichzeitig hoher Ansteckungsrate gab es weder Möglichkeiten zur effektiven Eindämmung der Pandemie noch zur Behandlung Betroffener. Der „Lockdown“ als einschneidende Maßnahme verursachte große finanzielle Schäden und Störungen im weltweiten Handel, die bis heute spürbar sind.

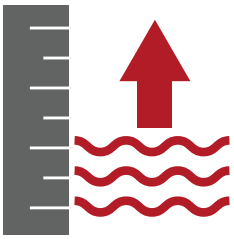


Mit der Pandemie einher ging eine Vielzahl an Herausforderungen:

Vielerorts waren Medizinprodukte unzureichend bevorratet. Zudem fehlten Pläne im Zusammenhang mit dem Ausfall größerer Teile der Beschäftigten bzw. der Fähigkeit, diese aus der Ferne arbeiten zu lassen. Außerdem mussten passende Impfstoffe entwickelt und zugelassen werden. Das liegt nicht zuletzt daran, dass es sich bei einer solchen Pandemie bis dahin um ein sehr abstraktes Bedrohungsszenario handelte. Sich auf alle (un)möglichen Fälle ausreichend vorzubereiten, ist schon aus Kostengründen nicht attraktiv. Es stellt sich also die Frage, wie mit der Vielzahl zumeist bedeutungsloser Warnungen umgegangen werden sollte und wie gleichzeitig die für die eigene Institution relevanten Bedrohungen erkannt und angemessen auf diese reagiert werden können.

Beispiel 2: Hochwasser und Starkregen

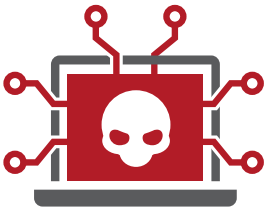
Bei der Flutkatastrophe im Ahrtal fielen große Teile der Infrastruktur aus. Im akuten Krisenfall war zunächst der Ausfall der Kommunikation besonders relevant – und das, obwohl sie auf den Notfall ausgelegt sein sollte. Doch die Basisstationen für Mobilfunk und das digitale BOS-Funksystem waren durch steigende Fluten von Strom- und Datenleitungen abgetrennt oder sogar ganz weggerissen. Die noch grundsätzlich betriebsbereiten Basisstationen waren überlastet und wenn Gespräche im Rückfallbetrieb möglich waren, erschwerten erhebliche Verzögerungen die Kommunikation. Grund dafür: Sichere Leitungen sind erheblich teurer als kommerziell verlegte Kabel. Die Behörden hatten deswegen das reguläre Netz gemietet.



Ohnehin sind Starkregenereignisse und Überflutungen typische unwahrscheinliche Ereignisse, bei denen klar ist, dass sie durch den Klimawandel zukünftig zunehmend zum Alltag gehören werden. Nur: Die jeweils betroffenen Gebiete lassen sich nicht vorhersagen. Kommunen können trotzdem auf vielfältige Arten vorsorgen. Die klassischen Ansätze in Form von Außengebietsentwässerung über die Vergrößerung des Kanalsystems bis hin zu Rückhalteanlagen werden zunehmend ergänzt um kleinteiligere Maßnahmen. Deren Ziel ist es, Wasser möglichst dezentral und großflächig verteilt aufzunehmen und langsam wieder abzugeben. Sinnbildlich wird dann von einer Schwammstadt gesprochen. Doch die zahlreichen Möglichkeiten, größere Schäden zu verhindern, basieren auf Prognosen zur maximal erwarteten Wassermenge. Wenn diese Menge überschritten wird, bilden effektive Notfallpläne, Gefährdungskarten und andere Vorsorgemaßnahmen die Grundlage, um im Ernstfall zügig handeln zu können.

Beispiel 3: Cyberangriffe

Massive Ausfälle durch Angriffe auf technische Infrastrukturen gelten noch immer als unwahrscheinliches Ereignis. Selten sind solche Angriffe jedoch nicht mehr. Allein im Jahr 2021 vermeldeten 27 kommunale Verwaltungen in Deutschland erfolgreiche Angriffe auf die IT-Infrastruktur. Betroffen waren kleine Gemeinden mit nicht viel mehr als 2.000 Einwohnern genauso wie Bochum und andere Großstädte. Der daraus resultierende Schaden stieg teilweise auf sechsstellige Summen an, mitunter waren Dienste gar monatelang nicht abrufbar. Und noch schlimmer: In manchen Fällen veröffentlichten Kriminelle empfindliche Daten im Darknet.



Das Problem: Kein IT-System kann mit 100%iger Sicherheitsgarantie vor Cyberattacken geschützt werden. Deswegen ist es umso wichtiger, vorbeugende Maßnahmen zum Schutz der Systeme zu treffen. Neben regelmäßigen Updates und einer netzwerktechnischen Trennung mit DMZ und Firewall sollte ein Notfallplan existieren, der festlegt, wann im Ernstfall welche Maßnahmen durch wen getroffen werden müssen. Auch die Sicherung der Daten durch Backups kann Schlimmeres verhindern.

Doch die Realität sieht manchmal anders aus: Viele Kommunen schützen sich nur unzureichend gegen Cyberattacken. Dabei liegt es oft nicht einmal an der fehlenden Sensibilisierung für dieses Thema. Stattdessen fehlen für die immer komplexer werdenden Anwendungen spezialisierte Fachleute. Dann sollte geprüft werden, ob Beschäftigte entsprechend fortgebildet und klare Zuständigkeiten definiert werden können. Wo anschließend immer noch administrative Lücken bestehen, sollte eine Zusammenarbeit mit anderen Kommunen, kommunalen Dienstleistern oder externen Spezialisten gesucht werden.

Weiter auf der folgenden Seite »

Menschliche Fehler machen unwahrscheinliche Ereignisse wahrscheinlicher

Sicherheitslücken können schon deshalb niemals ausgeschlossen werden, weil jede Software zu anderer Software und Hardware in Verbindung steht. Durch diese fast unendlichen Kombinationsmöglichkeiten können sich spezielle Risiken ergeben, die nur in sehr seltenen Fällen bestehen und daher vorab bei Qualitätstests nicht gefunden wurden. Es gibt jedoch noch eine weitaus größere Fehlerquelle: Menschliche Fehlhandlungen aus Bequemlichkeit, Unachtsamkeit, Überforderung oder sogar mit Vorsatz. Bei neun von zehn entdeckten Sicherheitslücken ist menschliches Handeln dafür zumindest mitverantwortlich.

Beheben lassen sich solche Probleme nur dadurch, dass jede Mitarbeiterin und jeder Mitarbeiter durch regelmäßige Schulungen sensibilisiert wird und notwendiges Grundlagenwissen erhält. Jeder und jedem muss klar sein, welche schwerwiegenden Konsequenzen ein Fehlverhalten nach sich ziehen kann. Denn alle müssen zum Schutz der IT-Sicherheit beitragen. Dies gilt umso mehr auch für diejenigen Personen, die über administrative Rechte verfügen. Sie müssen in die Lage versetzt werden, die ihnen anvertrauten Systeme und Anwendungen zu administrieren, Fehlkonfigurationen und Bedrohungen zu erkennen sowie angemessen darauf reagieren zu können. In diesem Zusammenhang ist es hilfreich, wenn in der Institution eine positive Fehlerkultur herrscht, bei der gemeldete Fehler und Sicherheitslücken honoriert werden und gemeinsam an deren Beseitigung gearbeitet wird.

Im Nachhinein betrachtet stellt sich mitunter heraus, dass auf den Führungsebenen gefallene Entscheidungen die Situation weiter verschärft oder sogar erst verursacht haben. So hätte möglicherweise eine teurere Kommunikationslösung bereits eine höhere Ausfallsicherheit geboten oder Cyberangriffe hätten möglicherweise abgewendet werden können, wenn Institutionen mehr Geld für die IT-Sicherheit zur Verfügung gestellt und entsprechende Notfallkonzepte erarbeitet hätten.

Anstatt sich in Diskussionen zu verlieren, wer was hätte besser machen müssen, sollten Vorfälle jedweder Art Anlass sein, daraus zu lernen und Maßnahmen zu ergreifen, mit denen ähnliche Ereignisse zukünftig verhindert oder zumindest besser bewältigt werden können.

Egal ob Führungskräfte ein Szenario falsch einschätzen oder Mitarbeiterinnen oder Mitarbeiter die falsche Entscheidung treffen: Menschliches Fehlverhalten ist immer möglich. Deswegen ist es umso wichtiger, auch auf unwahrscheinliche Notfälle vorbereitet zu sein und bei den Gegenmaßnahmen durch eine sorgsame Dokumentation den menschlichen Fehler möglichst auszuschließen. Denn gerade unter Druck neigen Menschen dazu, Fehler zu begehen. Hierzu gehört auch, ein täglich verwendetes Passwort oder einen Klick an entscheidender Stelle zu vergessen.

Wenn wir etwas aus der Corona-Pandemie und anderen unwahrscheinlichen Ereignissen lernen können, dann das: Es mag unattraktiv und unverhältnismäßig teuer erscheinen, sich auf das Unwahrscheinliche oder gar Unvorstellbare vorzubereiten. Planungen fühlen sich möglicherweise sinnlos an. Doch wenn ein unwahrscheinliches Ereignis eintritt und Notfallpläne in der Schublade liegen, helfen sie dabei, den Kopf freizuhaben für das Wesentliche: Überlebensnotwendiges zu retten.

Auf viele Szenarien vorbereitet

Es ist nicht möglich, sich optimal auf jedes unwahrscheinliche Ereignis vorzubereiten. Nicht zuletzt spielt der Kosten-Nutzen-Faktor eine wichtige Rolle: Es ist nicht wirtschaftlich, auf jeden unwahrscheinlichen Ernstfall einzugehen und Vorkehrungsmaßnahmen zu treffen. Die gute Nachricht: Das ist auch nicht notwendig. Denn es gibt einige Grundüberlegungen, die für nahezu jedes unwahrscheinliche Ereignis eine wichtige Rolle spielen und dabei helfen können, Schaden im Ernstfall abzuwenden. Hierunter fallen beispielsweise:

- **Sich einen Überblick über die wirklich wichtigen Prozesse verschaffen:**
  Welche Aufgaben, Tätigkeiten und Prozesse sind absolut notwendig und müssen deswegen funktionieren? Welche sind demgegenüber eher nachrangig?

- **Sich einen Überblick über den Schutzbedarf der eigenen Daten verschaffen:**
  Welche Daten und damit Systeme, Schnittstellen und Personen sind von großer Relevanz, damit die zuvor als besonders wichtig definierten Prozesse ablaufen können?

- **Sich über die Verfügbarkeitsanforderungen klar werden:**
  Wie schnell müssen Prozesse nach einem Ausfall wieder zur Verfügung stehen? Reicht es aus, wenn nur bestimmte Kernprozesse innerhalb eines definierten Zeitfensters (z. B. Stunden, Tage, …) zur Verfügung stehen? Gilt dies ständig oder vor allem zu bestimmten Zeiten wie beispielsweise dem Monatsende? Kann mit den vorhandenen technischen Mitteln eine Wiederherstellung innerhalb des gewünschten Zeitfensters sichergestellt werden?

- **Abstrakte Ausfallszenarien betrachten:**
  Gibt es z. B. Notfall- oder Ausweichszenarien bei Personal- bzw. Systemausfall, Netzwerkstörungen sowie Betretungsverbot der Räumlichkeiten? Kann auch auf gleichzeitig auftretende Ausfälle angemessen reagiert werden?

- **Die wesentlichen Informationen ausfallsicher verfügbar halten:**
  Existiert eine Dokumentation, die das Wiederanlaufen von Systemen und Prozessen erleichtert und systematisiert? Ist diese Dokumentation unter allen betrachteten Ausfallszenarien zugänglich und umsetzbar?

- **Den Notfall üben:**
  Können die Systeme auch bei Stromausfall genutzt werden bzw. fahren sie ordnungsgemäß herunter? Sind Zutritt und Zugang zu allen relevanten Bereichen und Systemen möglich? Kann ein System innerhalb des gewünschten Zeitfensters komplett wiederhergestellt werden? Ist die Dokumentation für ein spezielles Szenario nachvollziehbar und zielführend?

Wer diese Fragen für sich selbst ehrlich beantwortet, ist auf mögliche Ernstfälle vorbereitet, ganz gleich wie diese aussehen. Die eindeutige Prioritätensetzung und die Notfallszenarien sorgen dafür, dass den verantwortlichen Personen klar ist, wie sie handeln müssen und in welcher Reihenfolge. Die beste Planung ist jedoch ohne entsprechende Übungen im Zweifelsfall wertlos, wenn ein entscheidender Aspekt vergessen wurde. Führen Sie daher geplante sowie ungeplante Notfallübungen durch. Jeder während einer Übung entdeckte Fehler kann dazu beitragen, für den Ernstfall besser vorbereitet zu sein.

Gelebte Informationssicherheit ist also immer auch ein Stück Vorsorge für den Ernstfall. Im Alltag mögen die zahlreichen Sicherheitsvorkehrungen zunächst als Last empfunden werden. Doch es kann immer passieren, dass Kriminelle eine neue Lücke entdecken und diese ausnutzen. Dann können genau diese Sicherheitsmaßnahmen den entscheidenden Unterschied machen, ob ein Angriff erfolgreich verläuft oder abgewehrt werden kann. Im Falle eines erfolgreichen Angriffs tragen die Notfallmaßnahmen dazu bei, so schnell wie möglich wieder arbeitsfähig zu sein.

Die Expertinnen und Experten der ITEBO-Unternehmensgruppe unterstützen Sie gerne dabei, ein effizientes Notfallmanagement zu etablieren. Auf diese Weise ist Ihr Unternehmen oder Ihre Verwaltung trotz Angriff so schnell wie möglich wieder arbeitsfähig.

ITEBO
Unternehmensgruppe
ganz nah

Kommunale Fachanwendungen und Datenschutz

Einführungsprojekte ganzheitlich gedacht

Datengetriebenes Verwaltungshandeln ist in kommunalen Gebietskörperschaften allgegenwärtig. Nicht selten werden hier sensible Daten von Bürgern verarbeitet. Jede Kommune ist gesetzlich verpflichtet, ihre Bürgerinnen und Bürger zu schützen: Auch und insbesondere vor Gefahren, die im Kontext eines etwaigen Datenmissbrauchs entstehen. Zunehmend komplexere Zusammenhänge bei eingesetzten Fachverfahren erschweren den Überblick für Kommunen, denn nicht jedes Fachverfahren behandelt ähnlich sensible Daten. Daraus ergeben sich teils sehr unterschiedliche Risikobewertungen, die mit ebenso unterschiedlichen Anforderungen einhergehen.

Datenschutz-Folgenabschätzung nach Risikoermittlung

Um eine Einschätzung des Risikos zu ermöglichen, ist es in einem ersten Schritt sinnvoll, einen Blick auf alle etwaigen Risiken zu legen. Dafür müssen die verantwortlichen Personen Geschäftsprozesse durchleuchten, eingesetzte IT-Systeme hinterfragen und die Ergebnisse dokumentieren. Ergibt diese Risikobetrachtung ein voraussichtlich hohes Risiko, besteht die **gesetzliche Verpflichtung**, für die entsprechenden Verarbeitungen **vorab** eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen.

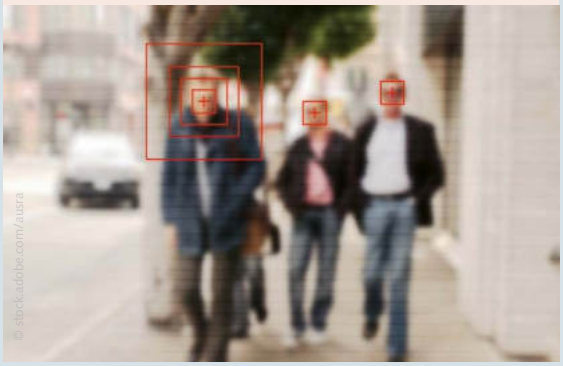
Eine DSFA dient dazu, potenzielle Risiken einer Verarbeitung personenbezogener Daten zu ermitteln und zu dokumentieren. Gleichzeitig werden die von der verantwortlichen Stelle zum Schutz dieser Daten getroffenen Maßnahmen bewertet. Idealerweise kommt man dabei zu dem Ergebnis, dass alle potenziellen Risiken durch die getroffenen Maßnahmen auf ein vertretbares Risikoniveau reduziert werden konnten. Sollte sich jedoch weiterhin ein hohes Risiko ergeben, müssen – falls möglich – die Schutzmaßnahmen verstärkt werden. Im ungünstigsten Fall kann es dazu kommen, dass trotz aller denkbaren umgesetzten Maßnahmen weiterhin ein hohes Risiko bei der Verarbeitung besteht. In diesem Fall muss entweder die Aufsichtsbehörde konsultiert oder die Verarbeitung eingestellt werden.

Weiter auf der folgenden Seite »

Risiko ist nicht gleich Risiko: So funktioniert eine Risikobewertung

Eine DSFA müssen Verantwortliche durchführen, wenn eine Risikobewertung ein hohes oder sehr hohes Risiko für die Betroffenen ermittelt. Maßgeblich für die Bewertung sind die Eintrittswahrscheinlichkeit und die Schwere des möglichen Schadens. Sie werden jeweils in „normal“, „hoch“ oder „sehr hoch“ klassifiziert. Beide Aspekte sind zur Bewertung notwendig, weil sie deutliche Auswirkungen nach sich ziehen.

Dies verdeutlicht das Beispiel einer Anschrift: Sie hat einen geringen Schutzbedarf, weil Personen üblicherweise kein Schaden entsteht, wenn diese öffentlich bekannt wird. Anders verhält sich dies bei Zeugen oder sogar verdeckten Ermittlern. Die Verknüpfung mit dieser zusätzlichen Eigenschaft führt sogar zu einem sehr hohen Schutzbedarf, da hierbei ein Datenmissbrauch die persönliche Unversehrtheit bedroht.



© stock.adobe.com/ausra

Darüber hinaus gibt es auch Daten mit einem hohen Schutzbedarf, der aus einem möglichen wirtschaftlichen oder gesellschaftspolitischen Ruin resultiert. Darunter fallen beispielsweise Steuerdaten, Personaldaten oder strafbare Handlungen.

Besonders aufmerksam müssen Verantwortliche nach EU-Richtlinien sein, wenn mindestens zwei als besonders riskant eingestufte Kriterien bei einem Datensatz erfüllt sind. Darunter fallen Scoring und Evaluierung, systematische Beobachtung und sensible Daten. Auch bei Datenverarbeitung in großem Umfang, automatisierter Entscheidung mit rechtlicher Wirkung oder Daten von besonders schutzbedürftigen Personen können spezifische Risiken entstehen. Äußerst vorsichtig müssen Verantwortliche auch dann sein, wenn Betroffene ohne die vorgeschaltete Datenverarbeitung nicht in der Lage wären, eine Dienstleistung oder ein Recht zu nutzen.

© stock.adobe.com/Irina Strelnikova

Zu den möglichen Schäden, die aus dem Datenmissbrauch resultieren können, zählen Diskriminierung, Rufschädigung, Identitätsdiebstahl oder finanzieller Verlust sowie Profilbildung mit Standortdaten und die verhinderte Kontrolle über eigene Daten.

Maßnahmen können Risiko senken

Ein hoher Schutzbedarf allein führt jedoch nicht zu einem hohen Risiko: Die Eintrittswahrscheinlichkeit ist ein weiterer wichtiger Faktor. Wer die Eintrittswahrscheinlichkeit verringert, kann auch das Risikoniveau für sensible Daten reduzieren.

Die ITEBO-Unternehmensgruppe ist Experte für Maßnahmen, die das Risiko senken – unabhängig davon, in welcher Stärke sie benötigt werden. Sie führt Datenschutzschulungen durch, entwickelt Notfallkonzepte und hilft dabei, klare und umsetzbare Regelungen zum Datenschutz zu etablieren. Außerdem schützt sie die Systeme ihrer Kunden durch moderne Maßnahmen wie Firewalls, Virenscanner oder Verschlüsselung und führt stetige Aktualisierungen durch.

© stock.adobe.com/RDBird

Risikobewertung im Optimalfall vor Projektbeginn beachten

Vereinfacht heißt dies: Planen Sie die Einführung einer neuen Software, ist stets die Dimension des Datenschutzes mitzudenken. Vor Projektbeginn!

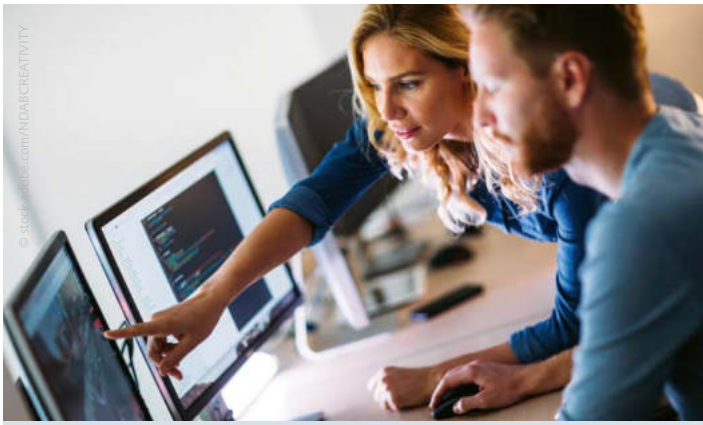
Entsprechende DSFAs sind darüber hinaus in jedem Fall ratsam: Vorsorge ist auch im Kontext von Datenschutz stets besser als reaktives Handeln.

Hierzu stellt Majid Cirousse fest: „Kunden unterschätzen nicht selten im Vorfeld von Softwareeinführungsprojekten die Zeit, welche für datenschutzrechtliche Belange eingeplant werden sollte. Projektverzögerungen und ungeplante Mehraufwände sind die Folge. Aufgrund unserer langjährigen Erfahrung im kommunalen Produktumfeld bieten wir eine umfassende Betreuung und gewährleisten die Berücksichtigung aller relevanten Datenschutzbelange."

Datenschutzbehörden liefern schon im Vorfeld Orientierung

Für viele Arten der Datenverarbeitung müssen die Risikobewertungen nicht durchgeführt werden, weil das Risiko bereits als so hoch eingeschätzt werden kann, dass Schutzmaßnahmen obligatorisch sind. Klarheit bieten die sogenannten Blacklists, mit denen Aufsichtsbehörden für Datenschutz arbeiten. Auf diesen Blacklists sind alle Datenverarbeitungen vermerkt, die grundsätzlich ein hohes Risiko aufweisen. Bei diesen Verarbeitungstätigkeiten ist es unumgänglich, eine DSFA durchzuführen.

Gelegentlich veröffentlichen die Behörden zudem auch Whitelists, auf denen Verarbeitungsarten enthalten sind, die nie hochrisikobehaftet sind. Besonderheiten ergeben sich dabei durchaus auch in einigen kommunalen Handlungsfeldern: So gehören zu den Kriterien, bei denen zwingend eine DSFA durchgeführt werden muss, die Verarbeitungsvorgänge auf der gemäß Art. 35 Abs. 4 DSGVO von der niedersächsischen Aufsichtsbehörde veröffentlichten (Muss-)Liste. Auf dieser ist u. a. die Verarbeitung von Meldedaten enthalten.



ITEBO-Unternehmensgruppe als erfahrener Datenschutzexperte für Kommunen

Die ITEBO-Unternehmensgruppe ist langjähriger erfahrener Dienstleister im Kontext kommunaler Fachanwendungen. Als Integrator und technischer Betriebsdienstleister unterschiedlicher Fachverfahren verfügt die ITEBO-Unternehmensgruppe neben dem datenschutzrechtlichen Know-how ebenfalls über die notwendige kommunale Prozess- und IT-Kenntnis.

„Unsere Fachberaterinnen und Fachberater, IT-Admins und die verantwortlichen Projektleiterinnen und Projektleiter stellen sich im Rahmen der Einführungsprojekte kommunaler Fachanwendungen ganz auf die Wünsche unserer Kunden ein. So ist es bereits vor Projektbeginn möglich, auf das gefragte Know-how der ITEBO-Datenschutzexperten zurückzugreifen", stellt Frederik Domain, Servicebereichsleiter im Bereich Bürgermanagement II dar. „Für Kunden kann dabei die Projektleitung des Softwareeinführungsprojektes als Single Point of Contact fungieren. Ganz im Sinne des Kunden entfällt somit langwieriger Abstimmungsbedarf zwischen den unterschiedlichen Gewerken."

Die Synergieeffekte sind sofort spürbar: Kurze Dienstwege sowie eine enge Abstimmung innerhalb der ITEBO-Unternehmensgruppe bringen erlebbaren Kundenmehrwert und schaffen schon zu Beginn das gute Gefühl, „an alles gedacht zu haben".

Datenschutzrechtliche Handlungssicherheit beim Einsatz neuer IT-Systeme erzeugt größtmögliche Sicherheit für die Daten der Bürgerinnen und Bürger. Dadurch können Kommunen den anstehenden Überprüfungen ihrer Datenschutzmaßnahmen gelassen entgegensehen.

Erfolgsfaktor des Datenschutzes

Bereichsübergreifende Zusammenarbeit maßgeblich

Eines der wichtigsten Ziele der ITEBO-Unternehmensgruppe ist es, ihre Kundinnen und Kunden durch eine qualitativ hochwertige Beratung mit ausgereiften und zuverlässigen Produkten jederzeit bestmöglich zu unterstützen. Dafür bündelt die ITEBO-Unternehmensgruppe ihre Kompetenzen bereichsübergreifend und stimmt sich intern ab.

Ganzheitliche Dienstleistungen anzubieten, obwohl ein bestimmter Servicebereich vermeintlich nicht beteiligt ist, gelingt nur durch die bereichsübergreifende Arbeitsweise. Diese Ganzheitlichkeit leben die ITEBO-Mitarbeiterinnen und -Mitarbeiter immer, doch selten ist dies so leicht verständlich und anschaulich wie bei den Themen Datenschutz und IT-Sicherheit. Denn beide Themen müssen immer mitgedacht werden, um (rechts-) sichere Dienstleistungen anbieten zu können.

Datenschutz und IT-Sicherheit müssen Kommunen, kirchliche Einrichtungen und Unternehmen bei jeder IT-Dienstleistung im Hinterkopf behalten. Das bedeutet für die ITEBO-Unternehmensgruppe, dass jeder Servicebereich auf diese Anforderungen eingestellt sein muss.

Die besondere Wichtigkeit der grundlegenden Kompetenzen führt Henning Köster, Servicebereichsleiter der ITEBO, aus: „Die Einhaltung des Datenschutzes ist gleichbedeutend mit Gesetzeskonformität und muss daher Teil jeder unserer Dienstleistungen sein. Das umfasst die Erfüllung der Informationspflichten (Bereitstellung von Datenschutzhinweisen) und den Abschluss von entsprechenden Verträgen zur Auftragsverarbeitung bis hin zur (optionalen) Durchführung kompletter Datenschutz-Folgenabschätzungen. Beides sollte für jeden Service bereitgestellt werden können."

Grundlegendes Verständnis immer vorhanden

Deswegen führt die ITEBO-Unternehmensgruppe intern regelmäßig die Sensibilisierung aller Beschäftigten in Bezug auf den Datenschutz durch. Ziel ist es, dass jede ITEBO-Mitarbeiterin und jeder ITEBO-Mitarbeiter die Anforderungen des Datenschutzes kennt. Die Beschäftigten werden dafür eingehend in Bereichen wie Datensparsamkeit, Nachweispflichten, technischen und organisatorischen Maßnahmen sowie im Umgang mit von Kundinnen und Kunden bereitgestellten Daten geschult.

So erreicht das Unternehmen, dass in allen Abteilungen ein grundsätzliches Verständnis zum Thema Datenschutz herrscht. Dadurch können die Expertinnen und Experten für andere Servicebereiche bereits grundsätzlich auf datenschutzrechtliche Anforderungen hinweisen und wissen, wann es sinnvoll ist, die tiefer gehende Expertise aus dem Servicebereich Datenschutz und IT-Sicherheit heranzuziehen.

Weiter auf der folgenden Seite »

OpenR@thaus: Datenschutz mitgedacht

Deutlich wird die Wichtigkeit der bereichsübergreifenden Kompetenzen beispielsweise bei unserem Serviceportal OpenR@thaus. Es ermöglicht Kommunen, Prozesse der Verwaltung sowohl Bürgerinnen und Bürgern als auch Unternehmen digital zur Verfügung zu stellen. Natürlich spielt der Datenschutz dort eine gewichtige Rolle, denn bei der Nutzung werden teilweise sehr sensible Daten verarbeitet. Zugleich wird die Digitalisierung mit dem Onlinezugangsgesetz (OZG) vom Gesetzgeber forciert, denn Kommunen, Länder und Bund müssen bis Ende 2022 ihre Verwaltungsleistungen auch digital anbieten. Insgesamt sind rund 600 Verwaltungsleistungen davon betroffen.

Die Liste an Dienstleistungen ist entsprechend lang und vielseitig. Sie reicht von der Beantragung von Altenhilfe bis hin zu Wohngeld, von der Ausgabe von Steuerunterlagen bis hin zu Zollangelegenheiten und von der Geburts- bis zur Sterbeurkunde. Die Kommunen müssen also viele Daten verarbeiten, deren Bekanntwerden für die Betroffenen ernste Konsequenzen haben könnte. Entsprechend wichtig ist es, dass der Datenschutz eingehalten und die Sicherheit der Daten gewährleistet wird.

Digitalisierung bietet Chancen

Doch die Digitalisierung von Prozessen bedeutet nicht nur eine hohe Verantwortung für die Kommunen. Im Gegenteil: Diese profitieren auch davon. Denn standardisierte Servicedienstleistungen bedeuten eine Arbeitserleichterung und zugleich eine beschleunigte Bearbeitung. Das führt zu einer erhöhten Zufriedenheit bei Mitarbeitenden, aber auch bei Bürgerinnen und Bürgern. Letztere nutzen den digitalen Zugang jedoch nur dann gerne, wenn sie davon ausgehen können, dass ihre Daten sicher sind. Der Datenschutz nimmt deswegen sowohl rechtlich als auch hinsichtlich der Zufriedenheit und der Akzeptanz durch Bürgerinnen und Bürger einen wichtigen Stellenwert ein.

Durchdacht digitalisierte Prozesse erhöhen die Datensicherheit sogar vielfach. So ermöglicht OpenR@thaus eine medienbruchfreie digitale Antragstellung und -bearbeitung. Das hat den „Nebeneffekt“, dass sich die Fehlerraten verringern und insgesamt ein erhöhtes Datenschutzniveau gewährleistet werden kann. Denn es gibt keine Umlaufmappen mit Anträgen mehr, die prinzipiell von jedem Mitarbeiter und jeder Mitarbeiterin eingesehen werden könnten. Stattdessen ist der Zugriff auf Anträge und deren Bearbeitung durch beschränkte Zugriffsrechte streng reglementiert.

© stock.adobe.com/SREDPIXEL

Datenschutz und OpenR@thaus: Von grundlegend bis spezialisiert

Die Standardisierung der Prozesse ermöglicht auch der ITEBO-Unternehmensgruppe, datenschutzrechtliche Aspekte bereits im Vorfeld mitzudenken und umzusetzen. Die Anforderungen der Kommunen an den Datenschutz sind dadurch sehr ähnlich und OpenR@thaus ist von Beginn an so datenschutzfreundlich wie möglich. Das bedeutet beispielsweise, dass bereits Datenschutzerklärungsmuster für die Prozesse vorliegen, die standardmäßig enthalten sind. Außerdem führt die ITEBO-Unternehmensgruppe mit ihren Kundinnen und Kunden einen Workshop vor Projektbeginn durch, in dem datenschutzrechtliche Fragestellungen durch die Expertinnen und Experten geklärt werden.

Doch nicht immer reicht eine standardisierte Lösung aus. Die ITEBO-Unternehmensgruppe führt die Integration weiterer OZG-Prozesse durch und bedenkt auch dabei datenschutzrechtliche Aspekte.

Ganzheitliche Sichtweise ermöglicht erfolgreiche Digitalisierung

Eine Lösung wie OpenR@thaus anzubieten, ohne die datenschutzrechtlichen Aspekte mitzudenken, wäre fahrlässig. Doch auch abseits der kommunalen Verwaltung zeigt sich immer wieder: Für die Kundinnen und Kunden der ITEBO-Unternehmensgruppe ist es unumgänglich, dass sie nicht nur technische Lösungen erhalten, sondern diese wichtigen rechtlichen Aspekte bereits bestmöglich abdecken. Wenn das nicht möglich ist, müssen Beraterinnen und Berater in der Lage sein, Unwägbarkeiten und besondere Bedarfe schon frühzeitig zu identifizieren und anzusprechen. Nur so können Prozesse effizient digitalisiert und Synergieeffekte tatsächlich nutzbar gemacht werden – ohne dabei die Belange Einzelner aus dem Blick zu verlieren.

Deswegen legt die ITEBO-Unternehmensgruppe viel Wert darauf, dass jeder Mitarbeitende immer auch ein bisschen Expertin oder Experte für Datenschutz ist. Oder zumindest weiß, wann mehr Fachwissen notwendig ist. Denn nur so können die Servicebereiche die qualitativ hochwertige und passende Beratung gewährleisten, die die ITEBO-Kundinnen und -Kunden so zu schätzen wissen.

Die Interoperabilität von OpenR@thaus ist immer auch eine Datenschutzfrage. Denn Bürgerinnen und Bürger müssen darüber informiert werden, wie die gespeicherten Daten verwendet werden können. Werden Servicekonten landesweit und kommunal genutzt, verändern sich die Ansprüche an die Datenschutzerklärungen und die Auskunftspflichten. Auch dies hat datenschutzrechtlich Vorteile für Bürgerinnen und Bürger. Sie können dann mit nur einem Konto zentral auf Dokumente und Anträge zugreifen. Zugleich haben sie nur noch einen und nicht viele Accounts, in denen sie Informationen über die Verarbeitung ihrer Daten erhalten. Es wird also deutlich einfacher für sie, ihre Rechte in Bezug auf den Datenschutz wahrzunehmen.

© stock.adobe.com/nenetus