05|2019
12. März
2. Jahrgang

sgp REPORT

DIE BASIS FÜR IHRE INVESTITIONEN IN DER SOZIALWIRTSCHAFT

schlütersche
www.sgp-report.de

BAUEN

INVESTIEREN

Soziale Wirtschaft

Aufbau eines neuen Diakonie-Konzern | **7**

Dealmaker

Ulrich Marseille first – wie der Unternehmer vom Verkauf profitiert hat | **14**

Angebote ausbauen

Ergebnisse einer Studie zu aktuellen Investitionsvorhaben der Branche | **16**

Risiko einpreisen

Nur angemessene Renditen sichern ein bedarfsgerechtes Betreuungs- und Pflegeangebot | **4**

BETREIBEN

Foto: Adobestock. Boris Zerwann

„Es kann jeden treffen!“

Ein Jahr DSGVO. Wie steht die Sozialwirtschaft zum Datenschutz und wen treffen Bußgelder? Und wie kann man sie vermeiden?

THOMAS ALTHAMMER IM INTERVIEW

In wenigen Wochen jährt sich die Einführung der Datenschutz-Grundverordnung (DSGVO) und das Inkrafttreten der neuen Kirchengesetze zum Datenschutz (DSG-EKD bzw. KDG) zum ersten Mal. Nach der anfänglichen Schonfrist häufen sich Berichte über Datenpannen und erste Bußgelder. Zum Stand der Umsetzung hat sgp REPORT bei Datenschutz-Experte **Thomas Althammer** nachgefragt.

Ist die Sozialwirtschaft beim Thema Datenschutz gut aufgestellt?

» Thomas Althammer: Bei unseren Mandanten schwankt die Stimmung zwischen Verunsicherung, Abwarten und Ernüchterung. Nach anfänglicher Hysterie haben sich viele Einrichtungen und Träger auf den Weg gemacht, die neuen Anforderungen in die Praxis umzusetzen. Es braucht aber noch Zeit, bis alle Vorgaben vollumfänglich abgearbeitet sind.

Wie steht es um die Motivation, gibt es ein Umdenken in Sachen Datenschutz?

» Althammer: Für uns als Datenschutzbeauftragte ist es deutlich einfacher geworden. Noch vor Jahren wollte niemand etwas dazu hören, obwohl die rechtlichen Rahmenbedingungen im Vergleich zur heutigen DSGVO bzw. den geltenden Kirchengesetzen ganz ähnlich waren. Das Thema wird ernst genommen und viele Unternehmen in der Sozialwirtschaft sehen beim Datenschutz mehr als nur die Erfüllung gesetzlicher Auflagen. Die neuen Bußgelder und Haftungsrisiken haben geholfen, dass das Thema ernster genommen wird.

„80.000 Euro Geldbuße, weil unbeabsichtigt sensible Gesundheitsdaten im Internet frei zugänglich waren.“

Thomas Althammer,
Althammer & Kill GmbH & Co.KG,
ta@althammer-kill.de,
www.althammer-kill.de

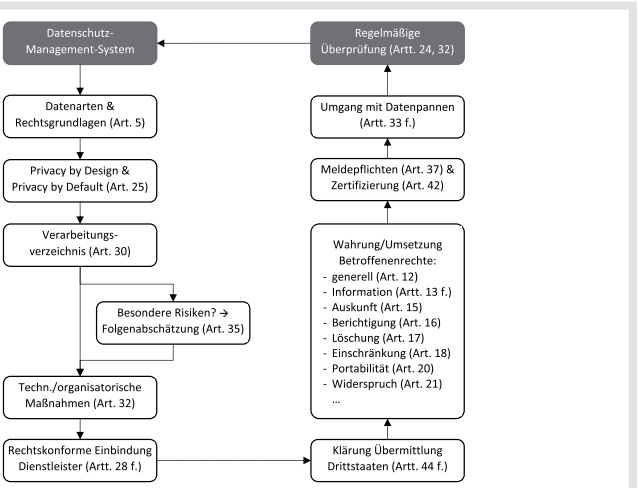
Foto: privat

Was müssen Unternehmen bei Datenschutzverstößen befürchten?

» Althammer: Die vielfach zitierten Bußgelder in Millionenhöhe sind als Strafmaß völlig unrealistisch in der Sozialwirtschaft. Derartige Beträge zielen eher auf internationale Konzerne wie Google oder Facebook ab, gegen die aktuell schon Verfahren laufen. Einen ersten Fingerzeig für unsere Branche gab es aus Portugal, als ein Krankenhaus im vergangenen Jahr mit einem Bußgeld von 400.000 EUR belegt wurde. Hintergrund war ein völlig unzureichendes Berechtigungskonzept, das vielen Benutzerkonten weitreichende Zugriffe gestattete. Der Fall soll noch gerichtlich geklärt werden.

Gibt es ähnliche Fälle in Deutschland?

» Althammer: Ja, in Baden-Württemberg sind beispielsweise schon Geldbußen ausgesprochen worden. 80.000 EUR wurden fällig, weil unbeabsichtigt sensible Gesundheitsdaten frei im Internet zugänglich waren. Wer meint, das könnte das eigene Unternehmen nicht betreffen, weil doch alles sicher auf Servern im eigenen Keller lagert, der irrt: Einfachste Konfigurationsfehler können dazu führen,



Vorgehensmodell zur Umsetzung der DSGVO-Vorgaben (in ähnlicher Weise relevant für DSG-EKD und KDG)

Abb.: Althammer

dass Daten unberechtigt eingesehen werden. Wir sind heute bereits sehr weitreichend vernetzt.

Behördenvertreter haben zuletzt angekündigt, dass es auch um fünf- und sechsstellige Geldbeträge gehen wird. Die Praxis zeigt leider, dass es jeden treffen kann, vom kleinen Pflegedienst bis zum großen Träger. Fast täglich werden wir mit Datenpannen bei unseren Kunden konfrontiert oder stoßen auf unzureichende Schutzmaßnahmen.

Wo lauern typische Gefahren in der Sozialwirtschaft?

» Althammer: Träger und Einrichtungen im Gesundheits- und Sozialwesen sind besonders exponiert. Die Budgets für IT-Sicherheitsmaßnahmen sind in unserer Branche vergleichsweise niedrig. Die Ausgaben für IT machen in der Regel nicht mehr als 1-1,5 % des Jahresumsatzes aus. Zum Vergleich: Im Bereich der Versicherungen wird je nach Sparte das Zwei- bis Dreifache in IT-Maßnahmen inkl. IT-Sicherheit investiert. Gleichzeitig fallen in der Sozialwirtschaft fast ausschließlich hoch sensible personenbezogene Daten an. Es braucht vielfach pragmatische Konzepte, um dem Schutzbedarf dieser Daten mit den technischen und finanziellen Möglichkeiten gerecht zu werden.

IT-Administratoren geben sich große Mühe, die Arbeitsabläufe in Pflege und Betreuung bestmöglich zu unterstützen. Häufig fehlt es an Zeit und einem durchgehenden Konzept für die regelmäßige Bewertung und Überprüfung von IT-Sicherheitsfragen.

Können Sie Beispiele benennen?

» Althammer: Da fällt mir ein Unternehmen der Sozialwirtschaft ein, dass mir stolz seinen biometrisch abgesicherten Zugang zum Serverraum zeigte, um die Daten der rund 3.000 Klienten zu schützen. Auf den ersten Blick eine tolle Lösung, war doch der Zutritt zu zentralen IT-Systemen gut abgeschirmt und kontrolliert. Erst auf den zweiten Blick fiel auf, dass der Backup-Server mit sämtlichen Daten wenige Kilometer weiter im Zimmer des Hausmeisters einer Einrichtung untergebracht war. Der Raum war meist unverschlossen und nicht besonders im Schließkonzept berücksichtigt.

Erst kürzlich wurde bei einem Mandanten ein Notebook mit sensiblen Klientendaten entwendet, die unverschlüsselt auf der Festplatte gespeichert waren. Das wird wahrscheinlich ein Bußgeld nach sich ziehen.

Also sollte man derartige Fälle besser für sich behalten?

» Althammer: Die DSGVO sieht eine gesetzliche Meldepflicht innerhalb von 72 Stunden vor. Vergleichbare Regelungen gibt es in den beiden Kirchengesetzen zum Datenschutz. Unterbleibt die Meldung oder wird erst verzögert die Aufsichtsbehörde informiert, ist auch hier ein Bußgeld fällig. Melden Sie lieber selbst, bevor es andere für Sie tun. In den vergangenen Monaten treten verstärkt Mitarbeitende und Kunden mit Beschwerden an Aufsichtsbehörden heran.

„Es geht um das kontinuierliche Bearbeiten und Verbessern datenschutzrechtlicher Belange."

Thomas Althammer

Der Experte ist als externer Datenschutzbeauftragter für Einrichtungen und Träger im Gesundheits- und Sozialwesen tätig.

Viele Einrichtungen fragen sich, ob das Erforderliche im Datenschutz getan ist. Wo sind typische Lücken und in welcher Reihenfolge sollte ich bei der Abarbeitung am besten vorgehen?

» Althammer: Die Grundzüge der DSGVO erinnern an die Vorgehensweise in QM-Systemen. Es geht also weniger um eine einmalige Abarbeitung, als vielmehr um ein kontinuierliche Bearbeitung und Verbesserung der datenschutzrechtlichen Belange. Dabei empfiehlt es sich – gemessen an der Prüfpraxis der Behörden und sich ergänzenden Anforderungen – schrittweise und planvoll vorzugehen (*s. Kasten und Abb.*). ■

Weitere Informationen:
www.althammer-kill.de

Datenschutz – schrittweiser Aufbau

- Benennen Sie eine/n Datenschutzbeauftragte/n
- Schulen Sie Ihre Mitarbeitenden zum Datenschutz (Schulung/Merkblätter) und verpflichten Sie sie auf die Vertraulichkeit
- Legen Sie ein Verzeichnis verarbeiteter Datenarten und zugehöriger Rechtsgrundlagen an
- Erstellen Sie ein Verzeichnis von Verarbeitungstätigkeiten
- Erstellen Sie ein Verzeichnis von technischen und organisatorischen Maßnahmen
- Führen Sie, bei entsprechenden Risiken (z. B. Videoüberwachung, Klientendokumentation), eine Datenschutz-Folgenabschätzung durch
- Informieren Sie Klienten, Angehörige und Mitarbeiter zur Datenverarbeitung und kommen Sie auf Anfrage den weiteren Betroffenenrechten nach
- Regeln Sie Prozesse zur Bearbeitung einer Datenpanne mit Meldung innerhalb von 72 Stunden
- Dokumentieren Sie die Einhaltung der Vorgaben in einem Datenschutzkonzept
- Überprüfen und aktualisieren Sie Impressum und Datenschutzerklärung auf Ihrer Homepage und bei Ihren Social Media-Aktivitäten