SOZIAL WIRTSCHAFT aktuell

sozialwirtschaft.nomos.de

8 | 2024
Mai

Infodienst für das Management in der Sozialwirtschaft

Vermeidung von Haftungsfallen:

Wer haftet bei Datenschutzverstößen nach der DSGVO?

Arne Wolff

Datenschutz und IT-Sicherheit stehen bei den meisten Organisationen nicht ganz oben auf der Prioritätenliste, werden aber vor dem Hintergrund der zunehmenden Digitalisierung in Verbindung mit immer unübersichtlicheren und komplexeren IT-Systemen immer wichtiger. Verstöße werden im Hinblick auf die Regelungen aus der Datenschutzgrundverordnung (DSGVO) scharf geahndet. Die Haftungsrisiken schließen sowohl das Management als auch Mitarbeitende mit ein. Vor dem Hintergrund, dass einerseits Cyber-Kriminalität in den letzten Jahren sprunghaft angestiegen ist (die IT-Sicherheitslage ist dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge angespannt bis kritisch) und sich andererseits die Datenverarbeitung und -speicherung über Cloud-Computing und Web-Applikationen immer weiter ins World-Wide-Web verlagert, wird klar, dass Handlungsbedarf besteht, sensible Unternehmensdaten wirkungsvoll zu schützen.

Welche Anforderungen ergeben sich aus der DSGVO?

Je nachdem, wie die Organisation strukturiert ist – z. B. über eine evangelische, katholische oder weltliche Trägerschaft – ergeben sich andere Prioritäten. Durch die Regelungen der DSGVO, des Bundesdatenschutzgesetzes, des Kirchengesetzes über den Datenschutz der Evangelischen Kirchen (EKD) oder des Gesetzes über den Kirchlichen Datenschutz (KDG) hat sich Datenschutz als integraler Bestandteil der Unternehmens-Compliance etabliert. Viele Anstrengungen wurden unternommen, den gesetzlichen Anforderungen Genüge zu tun. Trotzdem steigt die durchschnittliche Höhe der Geldbußen aufgrund von Verstößen gegen die DSGVO seit 2019 kontinuierlich an.

Zum einen können Geschädigte nach Art. 82 DSGVO einen Schadenersatzanspruch geltend machen – und zwar gegenüber dem Verantwortlichen, also dem Unternehmen. Zum anderen können die zuständigen Aufsichtsbehörden nach Art. 83 DSGVO Bußgelder verhängen. Zum Beispiel aufgrund von

- Verstößen gegen die Grundsätze der Datenverarbeitung (Art. 5,6,7 und 9 DSGVO)
- Verstößen gegen die Rechte der betreffenden Personen (Art. 12 bis 22 DSGVO)
- Verstößen bei der Übermittlung personenbezogener Daten in ein Drittland [Stichwort: Umgang mit Microsoft 365] (Art. 44 bis 49 DSGVO)

Art. 5 DSGVO legt fest, dass personenbezogene Daten so verarbeitet werden müssen, dass ihre Integrität und ihre Vertraulichkeit gewährleistet sind und der Verarbeiter darüber Rechenschaft ablegen kann. Um dies zu erreichen, verpflichten Art. 24 und 25 DSGVO dazu, geeignete technische und organisatorische Maßnahmen zu ergreifen und verlangen deren risikobasierte Auswahl unter Betrachtung der Rahmenbedingungen. Art. 32 DSGVO schließlich ergänzt ein weiteres Schutzziel: die Verfügbarkeit der Daten. Nun gilt die DSGVO zwar grundsätzlich nur für die Verarbeitung personenbezogener Daten, aber auch in anderen Rechtsbereichen ist vorgeschrieben, dass die

In dieser Ausgabe

Nomos

Nomos eLibrary

https://doi.org/10.5771/1619-2427-2024-8-1-1

Sicherheit bei der Verarbeitung von Daten gewährleistet wird (Gesellschaftsrecht, Haftungsrecht, Bankenrecht und andere). Und nicht zuletzt verlangen auch die Anbieter der zunehmend populärer werdenden Cyber-Versicherungen in der Regel ein Mindestmaß an Informationssicherheit.

Warum gehören Datenschutz und Informationssicherheit zusammen?

Die Ziele des Datenschutzes gehen mit denen der Informationssicherheit Hand in Hand. Das eine kann es ohne das andere nicht geben.

- **Vertraulichkeit der Daten:** Es muss dafür gesorgt werden, dass nur die Informationen zugänglich sind, die gebraucht werden.
- **Integrität der Daten:** Ihre Verlässlichkeit ist in vielen Bereichen lebenswichtig, etwa bei der Dosierung von Medikamenten. Dabei kann sowohl menschliches als auch technisches Versagen zu unabsichtlichen Änderungen führen – beides gilt es zu berücksichtigen.
- **Verfügbarkeit der Daten:** Kaum ein Tag vergeht, an dem nicht gemeldet wird, dass es wieder ein Unternehmen erwischt hat: Ransomware. Ein unbedachter Mausklick, und ein Verschlüsselungsalgorithmus tut seine kriminelle Arbeit – die Daten sind zwar noch vorhanden, aber ohne Passwort nicht mehr im Zugriff. Auch hier können die Folgen lebensbedrohlich sein.

Auch die finanziellen Schäden sind gravierend, bis Daten wieder zur Verfügung stehen, von den Reputationsschäden von Unternehmen und Organisationen ganz zu schweigen

Wie lassen sich die Ziele der Informationssicherheit erreichen?

Das BSI hat zu diesem Zweck eine „IT-Grundschutz[1]“ genannte Vorgehensweise entwickelt, die es ermöglichen soll, das angestrebte Schutzniveau strukturiert zu erreichen. Wichtigstes Werkzeug ist dabei das jährlich veröffentlichte „IT-Grundschutz-Kompendium[2]“, das gut 100 sog. Bausteine enthält, die jeweils einen relevanten Sicherheitsaspekt fokussieren und analog zu den technischen und organisatorischen Maßnahmen stehen, wie sie im Datenschutz geläufig sind:

- ISMS (Sicherheitsmanagement)
- ORP (Organisation und Personal)
- CON (Konzeption und Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion und Reaktion)
- APP (Anwendungen)
- SYS (IT-Systeme)
- IND (Industrielle IT)
- NET (Netze und Kommunikation)
- INF (Infrastruktur).

Glücklicherweise sind nicht alle Bausteine für jede Organisation relevant.

Bei der Umsetzung sollten sich Verantwortliche zuallererst einen Überblick verschaffen, welcher Ist-Zustand in der Organisation im Bereich der Informationsverarbeitung vorliegt und welches Sicherheitsniveau angestrebt werden soll („Schutzbedarfsfeststellung“). Danach gilt es, den bekannten **PDCA-Zyklus** umzusetzen:

1. **P**lan: Planung der Sicherheitsmaßnahmen,
2. **D**o: Umsetzung der Maßnahmen,
3. **C**heck: Erfolgskontrolle,
4. **A**ct: Beseitigung von Defiziten und Verbesserung der Maßnahmen und Prozesse).

Es lohnt nicht nur für große Sozialeinrichtungen, sich mit Datenschutz und Informationssicherheit zu beschäftigen und Maßnahmen zu ergreifen, die auf Integrität, Vertraulichkeit und Verfügbarkeit der eigenen Daten einzahlen. Insbesondere vor dem Hintergrund, dass auch der Gesetzgeber die Digitalisierung von immer mehr Prozessen vorantreibt – wie z.B. der digitalen Patientenakte.

Wenn der worst case eintritt - haftet die Organisation oder der Mitarbeitende?

Wie beschrieben, werden die zuständigen Aufsichtsbehörden gegenüber dem Verantwortlichen, also der Organisation, Bußgelder verhängen. Sind Personen vom Datenschutzverstoß betroffen, können auch diese Schadenersatz fordern. Mitarbeitende können nur im Innenverhältnis mit dem Arbeitgeber für solche Verstöße haften. Das Arbeitsverhältnis ist aus rechtlicher Sicht ein Schuldverhältnis mit gegenseitigen Rechten und Pflichten. Die Mitarbeitenden treffen dabei Sorgfaltspflichten; insoweit haben sie auch die Einhaltung datenschutzrechtlicher Vorgaben zu beachten. Verstoßen Mitarbeitende nun gegen die Vorgaben und verursachen dadurch einen Schaden beim Arbeitgeber, so können auch Mitarbeitende dem Arbeitgeber gegenüber haften, und zwar je nach Grad ihres Verschuldens:

- **Leichte Fahrlässigkeit:** Der Mitarbeitende haftet nicht. Es geht hier um geringfügige Verstöße, die jedem Mitarbeitenden im Laufe der Zeit passieren können.
- **Mittlere Fahrlässigkeit:** Der Mitarbeitende haftet anteilig. Der genaue Umfang der Haftung richtet sich nach Billigkeits- und Zumutbarkeitsgesichtspunkten. Dabei wird etwa die Höhe des Schadens, der Grad des Verschuldens, das Risiko der Tätigkeit, die Höhe des Arbeitsentgelts, die Versicherbarkeit des Risikos, aber ggf. auch persönliche Umstände berücksichtigt.
- **Grobe Fahrlässigkeit:** Der Mitarbeitende haftet grundsätzlich voll. Eine Haftungseinschränkung ist jedoch möglich, wenn der Verdienst des Arbeitnehmers in einem deutlichen Missverhältnis zum Schadensrisiko der Tätigkeit steht. Als Haftungsobergrenze werden dabei regelmäßig drei Bruttomonatsgehälter vorgeschlagen.
- **Vorsatz:** Der Mitarbeitende haftet vollumfänglich.

Der Grad der Fahrlässigkeit ist dabei immer eine Einzelfallentscheidung, denn die Gerichte berücksichtigen viele Einzelfaktoren und gewichten sie unter Umständen unterschiedlich. In einigen Sonderfällen kann der Mitarbeitende auch selbst Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO werden, etwa weil er eigenmächtig oder im eigenen Interesse handelt – das kommt aber eher selten vor.

Was ist im Fall eines Datenschutzverstoßes zu tun?

Im Fall von IT-Angriffen, Datenpannen, Erpressungsversuchen und Betriebsunterbrechungen ist professionelles, ruhiges, trainiertes und zielgerichtetes Handeln von wesentlicher Bedeutung. Im Vorfeld klar definierte Rollen- und Verantwortlichkeiten, Maßnahmen- und Notfallpläne, Wiederanlaufstrategien sowie vorbereitete Krisenkommunikationsmaßnahmen sind von wesentlicher Bedeutung für

eine wirksame Bewältigung des Ereignisses. Informationssicherheits- und Datenschutzbeauftragte müssen sich im Ernstfall schnell ein umfassendes und klares Bild über die Lage machen können.

Auch risikominimierende Maßnahmen zum Schutz der Betroffenen und um den Schaden einzudämmen, müssen unverzüglich umgesetzt werden. Von besonderer Bedeutung ist auch die Einhaltung der datenschutzrechtlich geforderten Meldefrist an die Aufsichtsbehörden; die Anforderungen der DSGVO sehen bei Datenpannen verschärfte Melde- und Informationspflichten an Aufsichtsbehörden und Betroffene vor. Sie erfordern eine zeitnahe Meldung an die jeweils zuständige Aufsichtsbehörde, zumeist innerhalb von 72 Stunden.

Bei neuen Erkenntnissen zu der jeweiligen Datenschutzverletzung muss der Aufsichtsbehörde darüber hinaus ein entsprechendes Update mitgeteilt werden. Zusätzlich bestehen unter Umständen Informationspflichten gegenüber den Betroffenen. Hierzu sind abgestimmte bereichsübergreifende Kommunikationsprozesse, z.B. zwischen Datenschutz, Compliance, Informationssicherheit, Unternehmenssicherheit, Revision, Kommunikationsabteilung und vor allem auch der Geschäftsführung zu empfehlen. Der Komplexität der Organisation und ihres IT-Informationsverbunds, des Ausmaßes der IT-Angriffe sowie auch mancher unbeabsichtigter, fahrlässiger Datenpreisgaben kann innerhalb einer Organisation nur im partnerschaftlichen Verbund der beteiligten Ressorts und Fachbereiche begegnet werden. Auch die Dokumentation sowie die Durchführung gerichtsverwertbarer interner forensischer Untersuchungen sind von entscheidender Bedeutung. Zusätzlich kann unter Berücksichtigung bestimmter Aspekte auch der Abschluss einer Cyber-Security-Versicherung von Vorteil sein.

Folgende Schritte sind im Ernstfall zu überprüfen:

1) **Lagebild:** Welches tatsächliche Schadensausmaß liegt vor und welche Systeme sind betroffen?
2) Welche **Sofortmaßnahmen** sind unmittelbar zu veranlassen?
3) Ist eine **Meldung** an die Datenschutzbehörde oder andere Stellen notwendig?
4) Ist eine forensische **Analyse** nötig?

5) Sind Maßnahmen zur **Beweissicherung** nötig?
6) Sind **Sicherheitsbehörden** zu involvieren?
7) Sind externe **Maßnahmen zur Krisenkommunikation** notwendig?

Vorsicht ist besser als Nachsicht – welche präventiven Maßnahmen minimieren die Risiken?

Zuallererst sind IT-Sicherheit und Datenschutz Chefsache. Wenn in der Geschäftsführung keine Sensibilität dafür vorhanden ist und damit keine Budgets und Ressourcen, kann Cyber-Security nicht funktionieren. Klar ist auch, dass es 100-prozentigen Schutz nicht geben kann. Dazu ist die fortwährende IT-Entwicklung viel zu schnelllebig. Es ist inzwischen keine Frage mehr ob, sondern nurmehr wann man Opfer eines Cyberangriffes wird. Deshalb sind strukturierte Bestandsaufnahmen und sich daraus ableitende Maßnahmenpläne essenziell. Allerdings fehlen allzu oft die Ressourcen.

Co-Managed Compliance & Security – was entlastet die Geschäftsführung?

Haftungsrisiken für die Geschäftsführung ergeben sich nicht nur aus der DSGVO. Deshalb ist es wichtig herauszufinden, welche rechtlichen Bestimmungen anwendbar sind und daraus für eine umfassenden Compliance ein Rechtskataster zu erstellen. Dort werden über Datenschutz und Informationssicherheit hinaus relevante Vorschriften gelistet, wie z.B. das Gleichbehandlungsgesetz, das Hinweisgeberschutzgesetz, die CSR-Pflicht, Datenschutzregelungen, das Gesetz über Ordnungswidrigkeiten, das GmbH-Gesetz (zwar sind viele Einrichtungen keine GmbHs, die Regelungen und Urteile dazu haben aber eine Ausstrahlungskraft auf andere Rechtsformen), das Mindestlohngesetz, Kündigungsschutzgesetz und viele weitere erfasst und unter anderem Aktualität und Verantwortlichkeiten sichergestellt.

Besonders in kleineren Organisationen sind Vollzeitstellen für Compliance, Informationssicherheit oder Datenschutz in der Regel nicht vorgesehen und nicht notwendig. Das heißt in der Praxis, dass ein Mitarbeitender diese Aufgaben „mit übernehmen muss“, was meist zu Schwierigkeiten führt. Es ist für Angestellte meist schwierig, den Finger in die Wunde zu legen und bei Vorgesetzten lang gel(i)ebte Prozesse in Frage zu stellen. Ein externer Berater kann eine gute Lösung sein. Dieser hat keine Scheu, Problemfelder anzusprechen und Lösungen anzubieten. Mit Externen können auch Synergieeffekte gehoben werden – man denke nur an Ver-

tretungsfähigkeit während Urlaubs- oder Krankheitstagen, laufende Fortbildung und Wissenstransfer aus breiter Praxiserfahrung. Externe kommen mit ihrem Background und Standing meist effektiver und effizienter zum Ziel.

Auch Technologie kann unterstützen. Ein komplexes Datenschutzmanagementsystem schießt für viele Organisationen ggf. über das Ziel hinaus, aber technische Lösungen machen vieles effizienter. Was man generell empfehlen kann, ist ein übergreifendes transparentes Meldeportal, in dem die Eingänge nach Kanal – also Rechtsgrundlage – sortiert werden und die den Organisationen im Hinblick auf umfassende Compliance Erleichterung verschaffen, den Überblick zu behalten. Dieses schließt Datenschutz und Informationssicherheit mit ein.

Schützt eine Cyber-Versicherung?

Um das finanzielle Risiko bei der Datenverarbeitung zu reduzieren, sind sog. Cyber-Versicherungen am Markt. Während nach herrschender Meinung in Deutschland Bußgelder nicht versicherbar sind, werden aber zahlreiche andere Kosten übernommen, die in Folge von Datenpannen und Cyberattacken auf ein Unternehmen zukommen können zum Beispiel:

- professionelles Krisenmanagement
- Datenwiederherstellung
- Kosten bei Betriebsunterbrechung
- Beauftragung externer IT-Forensiker
- Beauftragung von Fachanwälten zur Abwehr ungerechtfertigter Bußgelder
- Schadenersatzforderungen von Kunden
- PR/Callcenter
- Kreditschutz- und Kreditüberwachungsservices
- strafrechtliche Verteidigung.

Da diese Versicherungssparte noch sehr jung ist, unterscheiden sich die Produkte je nach Anbieter teilweise stark voneinander – also „Augen auf“ beim Vergleichen!

Als positiven Nebeneffekt einer solchen Versicherung kann man werten, dass die Versicherer in der Regel ein (umgesetztes) IT-Sicherheitskonzept voraussetzen und so ihre Kunden zwingen, einen gewissen Mindeststandard einzuhalten.

Fazit

Es lohnt sich für große, aber auch kleine Pflege- und Sozialeinrichtungen, sich mit Datenschutz und Informationssicherheit zu beschäftigen und Maßnahmen zu ergreifen, die Integrität, Vertraulichkeit und Verfügbarkeit der eigenen Daten absichern. Insbesondere vor dem Hintergrund, dass auch der Gesetzgeber die Digitalisierung von immer mehr Prozessen vorantreibt – wie z.B. der digitalen Patientenakte. Informationssicherheit lässt sich zwar auch mit anderen Methoden und Hilfsmitteln strukturieren, umsetzen und verbessern, der IT-Grundschutz des BSI ist aber ein Standard, der weit verbreitet und gut übertragbar ist. Im Weiteren kann etwa das bekannte ISO-27001-Zertifikat auf Basis des IT-Grundschutzes erlangt werden.

Quellen:

(1) *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html*

(2) *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.thml*

Autor

Arne Wolff©Christian Wyrwa

Arne Wolff

Berater für Datenschutz und IT-Sicherheit bei Althammer & Kill, Hannover.

67. Treffen der Behindertenbeauftragten Bund-Länder

15 Jahre ist die UN-Konvention über die Rechte von Menschen mit Behinderungen in Deutschland geltendes Recht. Im Sommer 2023 wurde ihre Umsetzung vom zuständigen Fachausschuss der UN geprüft. Das Ergebnis: Es besteht noch deutlicher Handlungsbedarf. Die Beauftragten des Bundes und der Länder für die Belange von Menschen mit Behinderungen haben nun in einer „Stuttgarter Erklärung“ einige ihrer zentralen Forderungen im Rahmen ihres 67. Treffens am 11. und 12. April 2024 veröffentlicht.

Zu diesen vier Themen nahmen die Beauftragten Stellung: Recht auf selbstbestimmte Lebensführung; Recht auf körperliche und seelische Unversehrtheit, Schutz vor Gewalt und Missbrauch; Ablehnung von Zwang; Partizipation auf allen staatlichen Ebenen.

Die „Stuttgarter Erklärung“ als PDF ist abrufbar unter: https://www.der-paritaetische.de/fileadmin/user_upload/Stuttgarter-Erklaerung_12-04-2024.pdf