EU-Datenschutz-Grundverordnung
ab 2018 bereits berücksichtigt

HAFTUNGSRISIKEN IN DER IT

Ein Leitfaden für Inhaber, Geschäftsführer und IT-Verantwortliche

IHK Schwaben

aitiRaum
Bestens vernetzt.

> DIE BEDEUTUNG VON CYBER-SECURITY NIMMT ZU UND IST NUR MIT STRUKTURIERTEM VORGEHEN ZU BEWÄLTIGEN.

Weitere Informationen zum Thema
Haftungsrisiken in der IT der IHK Schwaben finden Sie unter
www.digitalisierung-schwaben.de – Nr. 3525580

VORWORT

Informationssicherheit und Datenschutz beschäftigen uns täglich – gerade im Zeitalter der Digitalen Transformation. Wenn z. B. Public Cloud-Dienste genutzt werden, verlassen Daten die eigenen Rechenzentren und damit den direkten Einflussbereich. Ohne eine Verschlüsselung der Daten auf dem Weg und in der Cloud ist das für unternehmenskritische Daten undenkbar.

Die Bedeutung von Cyber-Security nimmt zu und ist nur mit strukturiertem Vorgehen zu bewältigen. In der Zusammenarbeit mit führenden Wissenschaftlern sind wir uns darin einig, dass Handlungsfelder definiert abgearbeitet werden müssen. Das gibt uns die Möglichkeit agil und flexibel zu agieren und Aufgabenpakete zu teilen oder gleichzeitig zu bearbeiten.

Mit dieser Broschüre schaffen wir für die Unternehmen einen zuverlässigen und praxisorientierten Leitfaden, der Orientierung und Sicherheit bietet und dieses strukturierte Vorgehen ermöglicht. Dafür den Initiatoren und Autoren vielen Dank. Nutzen Sie diese und die weiteren Informationsmöglichkeiten der Kooperation zwischen der IHK Schwaben und dem aitiRaum e. V. und nehmen Sie auch an den Treffen unseres CIO-Networks teil. Mit diesem Austausch bleiben Sie „up-to-date" und finden Antworten auf aktuelle und drängende Fragen.

Robert Mayer
Leiter CIO-Network IHK Schwaben
Head of ITG Central Europe
Information Technology Group (ITG), EMEIA
FUJITSU

INHALTSVERZEICHNIS

A. EINLEITUNG

Wenn Sie über Haftungsrisiken durch den Einsatz von Informationstechnologie und deren Absicherung nachdenken, ist entscheidend, eine klare Gliederung der Verantwortungsbereiche und Handlungsfelder festzulegen, mit der Haftungsrisiken so gut als möglich reduziert werden können.

B. VERANTWORTUNG

Die Absicherung von IT-Haftungsrisiken obliegt dem Vorstand bzw. der Geschäftsführung. Im schlimmsten Fall wird eine persönliche Verantwortung und Haftung möglich sein.

1. Sorgfaltspflichten des ordentlichen Kaufmanns

Dass die rechtliche Verpflichtung aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich herrührt, dass Vorschriften aus dem Aktiengesetz vgl. § 91 Abs. 2 und § 116 Aktiengesetz bzw. § 43 GmbHG sich an den Vorstand, Aufsichtsrat und Geschäftsführer mit den Sorgfaltspflichten des ordentlichen Kaufmanns richten, ist bekannt.

2. Risikomanagementsystem

Die Unternehmensleitung hat im Rahmen ihrer Sorgfaltspflicht ein Überwachungssystem einzurichten. Mit dem Überwachungssystem soll im Grunde der Fortbestand der Gesellschaft gesichert werden. Dieses Überwachungssystem ist nichts anderes als ein Risikomanagementsystem.

3. Haftungsbereiche als Compliance-Vorgaben

In der Risikovorsorge geht es immer im ersten Schritt darum, die einzelnen Haftungsbereiche zu lokalisieren. Eine gängige Aufteilung und Zuordnung der Compliance-Vorgaben ist die Darstellung nach strategischen, konzeptionellen und operativen Aufgaben.

4. Gesamtverantwortung

Auch wenn die Verantwortung für die IT-Systeme vielleicht nur einem Vorstandsmitglied zugeordnet wird, gilt der Grundsatz der Gesamtverantwortung, wenn andere Vorstandsmitglieder feststellen, dass rechtswidrige Handlungen stattfinden. Sie sind dann verpflichtet, eigenständig zu recherchieren und Rechtsverstöße aufzudecken.

C. STRATEGISCHE AUFGABEN

Als strategische Aufgabe wird die
1. Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung betrachtet, zudem
2. die Einführung einer Datenschutzorganisation mit Bestellung eines betrieblichen Datenschutzbeauftragten nach den Vorgaben des Bundesdatenschutzgesetzes und ab Mai 2018 nach den Vorgaben der Europäischen Datenschutz-Grundverordnung (EU-DS-GVO), siehe auch unter dem Kapitel E, Datenschutz-Compliance.

Den rechtlichen Hintergrund dafür bilden der vorbenannte § 91 Abs. 2 Aktiengesetz, § 43 GmbHG, für die Datenschutzorganisation, § 4f BDSG und künftig Art. 37 ff. Europäische-Datenschutz-Grundverordnung (EU-DS-GVO).

D. KONZEPTIONELLE AUFGABEN

Nachdem das Unternehmen entschieden hat, IT–Haftungsrisiken strategisch abzusichern, geht es als nächstes daran, konzeptionelle Aufgaben im Unternehmen abzuarbeiten.

1. Sicherheitskonzept und Datenschutzkonzept

Wiederum aus dem Grundsatz der IT-Risikovorsorge ist die Erstellung eines Sicherheits- und eines Datenschutzkonzeptes erforderlich.

a. Typischerweise werden im Zusammenhang mit Sicherheitskonzepten unterschiedliche Standards berücksichtigt. Je nachdem, welches Sicherheitsniveau das Unternehmen erreichen will, sind Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik, BSI Grundschutzkataloge, oder ISO Vorgaben, beispielsweise ISO 27001 zur Beschreibung von Sicherheitsstandards maßgebend. Teilweise folgen Anforderungen aus Konzernabhängigkeiten, teilweise verlangen Kunden oder Behörden entsprechende Sicherheitsstandards, die dann im Sicherheitskonzept abzubilden sind.

b. Angesichts der Vorgaben der Europäischen Datenschutzgrundverordnung (EU-DS-GVO) und des im Art. 5 Abs. 2 GVO geregelten Grundsatzes, dass das Unternehmen zum Stand der Datenschutzorganisation Rechenschaft gegenüber Datenschutzaufsichtsbehörden ablegen muss, ist die Erstellung eines Datenschutzkonzeptes wieder in den Fokus der konzeptionellen Aufgaben gelangt.

Hier wird es künftig darum gehen, die Vorgaben der EU-DS-GVO als Pflichtenheft darzustellen und umzusetzen.

Die GVO gilt ab dem 25. Mai 2018

Die GVO gilt ab dem 25. Mai 2018. Zur Prüfung, ob Handlungsbedarf besteht, sind vorhandene Prozessabläufe zu analysieren und der kommenden Gesetzgebung anzupassen. Aufgrund der Vielschichtigkeit der Vorgaben wird sowohl der zeitliche als auch der finanzielle Aufwand innerhalb der Datenschutzorganisation erhöht werden müssen.

Folgende Herausforderungen lassen sich zusammenfassen:

1. Der Betroffene hat nach der GVO ein erweitertes Informations- und Auskunftsrecht, insbesondere kann er die Datenübertragung aller über ihn gespeicherten Daten – auch Daten aus den Webservern – auf einen von ihm festgelegten neuen Dienstanbieter verlangen. Ihm steht nicht nur ein Recht zu, über die Dauer der Datenspeicherung informiert zu werden, sondern er hat auch ein Widerspruchsrecht, wenn seine Daten an Dritte weitergegeben werden sollen. Ferner steht ihm ein Beschwerderecht bei der Aufsichtsbehörde zu.

2. Von dem Verantwortlichen der Datenverarbeitung sind geeignete technische und organisatorische Maßnahmen zu implementieren, um die Einhaltung der GVO sicherzustellen. Dazu sind Datenschutzrichtlinien zu implementieren, Verhaltensregeln aufzustellen und die Einhaltung eines genehmigten Zertifizierungsverfahrens sicherzustellen, was als Nachweis von Compliance dient. Dazu werden die Aufsichtsbehörden entsprechende Leitlinien verfassen.

3. Die Gestaltung des Datenschutzes hat sich daran zu orientieren, dass möglichst eine Pseudonymisierung, eine Datenminimierung sowie eine erforderliche Zweckbestimmung (Menge, Umfang, Speicherfrist, Zugänglichkeit (=Privacy by default)) eingehalten wird.

4. Der Auftragsverarbeiter ist nach der GVO künftig auch Verantwortlicher und haftet demnach nun auch für die Unterauftragnehmer.

5. Kommt es zur Verletzung der Sicherheit personenbezogener Daten, so ist dies der Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Dazu werden die Aufsichtsbehörden entsprechende Leitlinien festlegen. Das Risiko kann reduziert werden, wenn geeignete technische und organisatorische Sicherheitsvorkehrungen, wie Verschlüsselung, für den Datentransfer genutzt werden. Falls nicht, ist über eine solche Datenpanne ein öffentlicher Aufruf notwendig. Die Verschlüsselung muss durchgängig auch von den Serviceprovidern eingehalten werden.

6. Jedes Verfahren, das eingesetzt wird, muss nach der GVO einer Datenschutzfolgeabschätzung (DSFA) unterworfen werden, wenn ein hohes Risiko für Rechte und Freiheiten von Personen besteht. Auch hier werden Leitlinien der Artikel 29 Gruppe entwickelt. Falls keine Maßnahmen zur Risikoreduzierung möglich sind, ist darüber mit der Aufsichtsbehörde eine Abstimmung herbeizuführen.

7. Um das Risiko internationaler Datenübermittlungen an Nicht-EU-Länder zu minimieren, sind bis auf weiteres EU-Standardvertragsklauseln der EU-Kommission oder Aufsichtsbehörde zu

verwenden. Für konzerninterne Übermittlungen können verbindliche Datenschutzrichtlinien festgelegt werden. Für Datenverkehre in die USA gilt das EU-U.S. Privacy Shield. Danach darf ein Datentransfer in die USA nur erfolgen, wenn das empfangende US-Unternehmen sich der Zertifizierung nach dem Privacy Shield unterworfen hatte.

8. Künftig haben die Aufsichtsbehörden die Möglichkeit, grenzüberschreitende Datenübermittlungen zu kontrollieren. Nach dem One-Stop-Shop ist die Aufsichtsbehörde federführend, an dessen Sitz sich die Hauptniederlassung eines Unternehmensverbundes befindet. Auch hier werden die Aufsichtsbehörden noch Leitlinien und Empfehlungen zur Verfügung stellen.

9. Nach der GVO haben Betroffene das Recht auf Beschwerde, gerichtlichen Rechtsbehelf sowie das Recht auf Schadenersatz, der auch immaterieller Art sein kann.

10. Künftig können Verstöße gegen Datenschutzregelungen durch Technik, DSFA, Verträge mit Service-Providern, fehlende Sicherheitsvorkehrungen, Mängel der Datenverarbeitungsverzeichnisse mit Geldbußen von bis zu 10 Mio. Euro bzw. 2 % des gesamten weltweiten Jahresumsatzes geahndet werden. Bei fehlenden Rechtsgrundlagen und illegalen internationalen Datenübermittlungen verdoppelt sich der Bußgeldbetrag. Dass im Unternehmensfokus neben der Erstellung von Sicherheits- oder Datenschutzkonzepten auch die ständige Aktualisierung oder Rückmeldung der Konzeptverantwortlichen sein muss, versteht sich von selbst. Bitte lesen Sie auch im Kapitel G die Empfehlung der Checkliste zur Umsetzung der Vorgaben der GVO.

2. Unternehmensdaten als Vermögenswert

Konzeptionell ist weiter der Zugang zu Unternehmensdaten, insbesondere personenbezogenen Daten durch externe Dienstleister oder Dritte zu regeln. Nachstehend eine kurze Skizzierung möglicher betroffener Bereiche:

a. Auftragsdatenverarbeitungsverträge oder Geheimhaltungsverträge

Es ist lediglich logische Konsequenz, dass je nachdem, ob der externe Dienstleister als Auftragsdatenverarbeiter tätig wird oder in eigener Regie Funktionen übernimmt, Auftragsdatenverarbeitungsverträge oder Geheimhaltungsverträge zu vereinbaren sind. Existenziell ist hier vor allem die Bewertung von Unternehmensdaten, die extern verarbeitet werden, wenn möglicherweise aus BigData-Anwendungen neues Datenmaterial mit enormem Vermögenswert entsteht. Zwingend müssen hier Eigentumsverhältnisse des Dateneigners, Urheber- und damit verbunden Nutzungsrechte, Rückgabepflichten und Löschfristen definiert werden.


Drag & Drop Files Here to Share
Select files to share
– meeting with Peter at 3 p.m. @ Coffee Bar
– marketing class start tomorrow
– buy new camera!

b. NDAs zum Start

Der Beginn einer Zusammenarbeit ist mit Geheimhaltungsvereinbarungen, sog. Non Disclosure Agreements (NDAs), zum frühestmöglichen Zeitpunkt zu regeln. Die Frage, welcher Schaden durch eine Vertragspflichtverletzung verursacht wurde, wenn der Dienstleister rechtswidrig wertvolles Datenmaterial nutzt, ist kaum sicher zu beweisen. Die logische Konsequenz sind Vertragsstrafen-Regelungen, die natürlich nicht wirksam vereinbart werden können, wenn pauschaliert bei Verstößen gegen den Gesamtvertrag formuliert wurde. Vielmehr sollte das Unternehmen bei Vertragsstrafen-Regelungen differenziert einzelne Pflichten mit Rahmenvertragsstrafsummen definieren, um wirksame Vertragsstrafen später durchsetzen zu können.

c. BigData und Cloud

In den nächsten Jahren wird der Umgang mit Dienstleistern und Vertragspartnern gerade bei BigData- und Cloud-Services, die nicht selten aus dem Ausland angeboten werden, in denen wertvolle Daten aus riesigen Datenbanken generiert werden bzw. wertvolle Daten weggegeben werden, für Unternehmen existenziell werden. Wer auf eine klare Abgrenzung von Rechten und Pflichten verzichtet, wird prinzipiell Sorgfaltspflichten des ordentlichen Kaufmanns verletzen.

d. Digitalisierung und Industrie 4.0

Viele rechtliche Fragen der Digitalisierung, den Anwendungsbereichen der „Industrie 4.0" lassen sich künftig nur über klare Gewährleistungsregeln, Service-Level-Agreements, Urheberrechts- und Nutzungsberechtigungen, Betriebs- und Geschäftsgeheimnisschutz und den rechtlich gesicherten Umgang mit personenbezogenen Daten von Betroffenen lösen.

e. Verletzung von Vertraulichkeit und Geheimhaltung

Hier sind die Rechtsgrundlagen sowohl im Zivilrecht wie im Wettbewerbsrecht verankert, übrigens sehr versteckt in § 17 UWG (Gesetz gegen den unlauteren Wettbewerb), wonach der Verrat von Betriebs- und Geschäftsgeheimnissen strafbar ist. In der Praxis wird meist vernachlässigt, dass die Antragsfrist für eine entsprechende strafrechtliche Verfolgung 3 Monate beträgt. Zudem lässt sich ein Betriebs- und Geschäftsgeheimnisverrat meistens auch wettbewerbsrechtlich sanktionieren und dies ohne die Beachtung dieser Frist von 3 Monaten.

3. IT-Beschaffung

Damit ist klar, dass die professionelle Beschaffung von IT-Systemen und die Durchführung von IT-Projekten ebenso Element der konzeptionellen IT-Risikovorsorge ist.

a. Rechtsgrundlage

Rechtsgrundlagen liegen hier im Zivilrecht, im Recht des Handelskaufs und des Werkvertragsrechts, wo Gewährleistungsfragen und Beweislastregeln verankert sind. Diese sind in IT-Projekten bei der IT-Beschaffung zu vereinbaren.

b. Auftragnehmer und Auftraggeber

Es besteht seit jeher ein Interessenskonflikt zwischen Software/Hardware-Anbietern als Auftragnehmer und Unternehmen, die entsprechende IT-Anschaffungen planen. Während die Auftragnehmer nach Aufwand abrechnen möchten, agieren Auftraggeber gerne mit Festpreisen zur Kalkulationssicherheit. Eine für beide Seiten befriedigende Fertigstellung des IT-Projekts lässt sich schon aus Prinzip nicht realisieren. Daher ist der für das auftraggebende Unternehmen entscheidende Faktor, über Zwischenschritte im Rahmen der Durchführung von IT-Projekten möglichst zeitnah Kostenveränderungen zu erkennen. Wichtige „Meilensteine" sind Vertragsanpassungs- oder dann Vertragsaustrittsklauseln, sog. „Change-Request-Management" und „Exit"-Regelungen.

E. OPERATIVE AUFGABEN

Nachdem strategisch und konzeptionell Haftungsrisiken begegnet wurde, ist die nächste Stufe der Absicherung die systematische Umsetzung verschiedener konkreter Aufgaben.

1. Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern

Zu den IT-Haftungsrisiken wird traditionell der Bereich der ordnungsgemäßen Buchführung betrachtet. Hier geben § 239 Abs. 4 HGB und das Steuerrecht, § 146 Abs. 5 Abgabenordnung die Grundlagen vor. In den letzten Jahren wurden diese Vorgaben als Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) weiter konkretisiert. Spätestens seit Januar 2015 haben diese Grundsätze auch die bekannten Grundsätze zum Datenzugriff und zur Überprüfbarkeit digitaler Unterlagen (GDPdU) und Grundsätze ordnungsgemäßer EDV-geschützter Buchführungssysteme (GoBS) abgelöst. In diesen neuen Regelungen sind die Vorgaben zur elektronischen Aufzeichnung der Barerlöse, Schutz vor Manipulation, umfassende Regelungen zum internen Kontrollsystem und der Verfahrensdokumentation besonders zu erwähnen.

2. Datenschutz-Compliance

Weitere operative Aufgabe ist der Aufbau der Datenschutzorganisation zur Gewährleistung der datenschutzrechtlichen Konformität. Dies beinhaltet die Umsetzung der Vorgaben aus Bundesdatenschutzgesetz, Telemediengesetz, sowie Wettbewerbsrecht, um Lieferantendaten, Kundendaten, Mitarbeiterdaten, die Personenbezug haben, zu schützen.

a. Datenschutzbeauftragte(r)

Kopf der Datenschutzorganisation ist der Datenschutzbeauftragte, der ab 10 Personen, welche regelmäßig personenbezogene Daten verarbeiten, zu bestellen ist.

b. Rechenschaftsverpflichtung nach der EU-DS-GVO

Wie schon erwähnt, bekommt die eingerichtete Datenschutzorganisation als sichtbare Gewährleistung der Umsetzung der Vorgaben der europäischen Datenschutzgrundverordnung neue Bedeutung. Nur durch den Betrieb und die Darstellung einer Datenschutzorganisation kann die Rechenschaftsverpflichtung aus der GVO, Art. 5 Abs. 2 EU-DS-GVO erfüllt werden, andernfalls drohen Bußgelder von bis zu 10 Mio. Euro bzw. bis zu 20 Mio. Euro. Hier erkennt der Leser aufgrund der Dimension der möglichen Bußgelder die Aufwertung der Datenschutz-Abteilung, die ähnliche Schutzvorkehrungen treffen muss wie Rechtsabteilungen der Unternehmen zur Abwehr von Kartellrechts-Verstößen. Lesen Sie daher unsere Empfehlung zur Planung der Umsetzung der Vorgaben der GVO im Kapitel G.

c. Untersagungs-Verfügungen

Seit jeher sind Aufsichtsbehörden rechtlich in der Lage, Datenverarbeitungsprozesse zu untersagen, wenn Verstöße gegen Datenschutzvorschriften lokalisiert wurden. Ganz zu schweigen von den neuen Programmfehlern aufgrund von Änderungsprogrammierung. Die frühzeitige Einbeziehung des Datenschutzbeauftragten, der Datenschutzorganisation dürfte daher bei der Planung von neuen Verfahren und neuer Software betriebswirtschaftlich deutlich sinnvoller sein.

3. IT-Sicherheit: Einsatz von Spam- und Virenfiltern

Um Cyberattacken abzuwehren und Schaden durch Vernichtung oder missbräuchlicher Verschlüsselung abzuwehren, ist die IT-Abteilung operativ zu beauftragen, Maßnahmen entsprechend zu ergreifen. Dies muss organisatorisch mit Nutzungsrechten der Mitarbeiter abgeglichen werden, damit nicht Vorgaben aus dem Fernmeldegeheimnis, vgl. § 88 TKG, oder Strafrecht, vgl. § 206 StGB betroffen sind, dazu aber im Folgenden mehr.

4. Internet- und E-Mailnutzung für Mitarbeiter

Dieses Thema ist seit Jahren Grund juristischer Auseinandersetzungen. Wichtig an dieser Stelle sind wenigstens folgende Aussagen: Es gibt keinen rechtlichen Anspruch, Mitarbeitern die private Nutzungsberechtigung der dienstlichen E-Mailadresse oder des dienstlichen Internet-Zugangs einzuräumen. Ein etwaiger Anspruch aus der von der Rechtsprechung quasi als „Gewohnheitsrecht" entwickelten betrieblichen Übung muss der Arbeitnehmer nachweisen, was eher nicht gelingen dürfte.

a. Entweder vollständiges Verbot der privaten Nutzung der betrieblichen IT oder nur Erlaubnis der privaten Nutzung des dienstlichen Internetzugangs

Die private Nutzung der dienstlichen Infrastruktur kann vollständig verboten werden. Alternativ kann die Nutzungsberechtigung auf die bloße private Internetnutzung beschränkt werden. Mitarbeiter verfügen meistens über mobile Geräte, mit denen Kommunikation möglich ist. Daher sollte eine Berechtigung, die dienstliche E-Mail-Adresse auch für private Zwecke nutzen zu dürfen, nicht erteilt werden. Alternativ kann die private Nutzung des dienstlichen Internet-Zugangs in angemessenem Umfang gestattet werden, dann können private E-Mail-Accounts über das Internet bedient werden, freilich nur, wenn Sicherheitsüberlegungen zum Betriebs- und Geschäftsgeheimnisschutz nicht entgegenstehen. Wichtig ist hier, dass eine Kontrollberechtigung bleibt.

b. Kontrollberechtigung muss bleiben

Ergebnis muss immer sein, dass entweder Kontrollmöglichkeiten schon kraft Gesetzes bestehen, wenn eine private Nutzung nicht erlaubt ist oder dann, wenn private Nutzung erlaubt wird, Mitarbeiter in entsprechende Kontrollmöglichkeiten auf Missbrauch einwilligen.

c. Problem: private Nutzung der geschäftlichen E-Mail-Adresse

Wird die private Nutzung der geschäftlichen E-Mailadresse erlaubt, muss zwingend im Rahmen einer Einwilligungserklärung durch Mitarbeiter vorab ein Herausgabeanspruch von archivierten privaten E-Mails ausgeschlossen werden. Ebenso muss die E-Mail-Weiterleitung im ungeplanten Abwesenheitsfall geregelt werden.

d. Einwilligung muss freiwillig erfolgen

Eine Einwilligung ist unter anderem nur dann wirksam, wenn sie freiwillig erteilt wurde. Freiwilligkeit kann nur vorliegen, wenn der Mitarbeiter eine Alternative hat, ohne Nachteile befürchten zu müssen. Dass eine entsprechende Einwilligung der Mitarbeiter freiwillig ist, ergibt sich daraus, dass der Mitarbeiter die Wahl hat zwischen der privaten Nutzung betrieblicher Einrichtungen, mithin Internet oder E-Mail, und bei fehlender Einwilligung oder Widerruf seiner Einwilligung dieser Mehrwert eben entfällt, er aber keine Nachteile hat.

5. Veränderung von Schädigung Dritter durch firmeneigene IT

Klar ist, dass durch die IT nicht Vertragspartner oder Dritte geschädigt werden dürfen. Die Schädigung Dritter ist sehr schnell passiert, wenn ein sicherer Versand nicht gewährleistet wird, Urheberrechte oder Vorgaben zum Direktmarketing nicht eingehalten werden. Typischerweise führen auch Rechtsverletzungen auf Webseiten zu Rechtsstreitigkeiten.

a. Sicherer Versand

Es muss ein virenfreier Datenaustausch gewährleistet werden. In diesem Zusammenhang


PRIVACY
Information
Systems
Protected

ist auch der Hinweis wichtig, dass über die datenschutzrechtlich unzulässige Weitergabe an unberechtigte Dritte in Mitarbeiterschulungen sensibilisiert werden muss, wenn Mitarbeiter an E-Mailverteiler in „CC:" anstatt in „BCC:" versenden oder falsche E-Mailempfänger als Adressaten von E-Mails auswählen.

b. Bildrechte Dritter
Über die Prüfung von Nutzungsrechten müssen Urheberrechte von Betroffenen oder Dritten gewährleistet werden. Werden Betroffene abgebildet, ist deren Einwilligung nach Kunst-Urheberrecht einzuholen.

c. Direktmarketing
Im Bereich Direktmarketing müssen datenschutzrechtliche und wettbewerbsrechtliche Vorgaben beachtet werden. Nur bestimmte Daten dürfen für personalisierte Briefwerbung verwendet werden, bei Telefon- und E-Mail-Werbung ist grundsätzlich eine ausdrückliche Einwilligung einzuholen, wobei im Bereich Geschäftskundenwerbung eine Telefonakquise leichter möglich ist und bei Bestandskunden durchaus eine Werbe-Kampagne per E-Mail unter bestimmten Bedingungen auch ohne Einwilligung funktioniert.

d. Online-Auftritt
Werden Online-Plattformen betrieben, Diskussionsforen oder Ähnliches unterhalten, sind Vorgaben des Telemediengesetzes, vgl. § 7 ff. TMG zur Störerhaftung für rechtswidrige Inhalte zu beachten. Die Vorgaben zum Telemediengesetz für Diensteanbieter und deren Webseiten insbesondere Impressumsangaben, Datenschutzerklärung, technisch organisatorische Absicherung der Kommunikation müssen gewährleistet werden.

6. Durchführung regelmäßiger Backups

Diese Forderung ergibt sich aus dem Prinzip der technisch organisatorischen Absicherung der IT- und Datenverarbeitung. Unterlassene oder mangelhafte Datensicherung kann zu einem Verstoß gegen den Grundsatz der IT-Risikovorsorge und zur persönlichen Haftung der Führungsebene führen.

7. Verwendung lizenzierter Software

Aufgrund der Vorgaben im Urheberrecht, hier § 94 ff. UrhG, haftet die Geschäftsführung persönlich bei wissentlichen Lizenzverstößen. Nicht selten besteht Unterlizenzierung dergestalt, dass weniger Lizenzen eingekauft wurden, als auf Arbeitsplatzrechner ausgerollt sind. Ein Lizenzmanagement ist zu empfehlen.

8. Cloud Computing

Nachdem die rechtliche Verantwortung für Absicherung von Datentransfers an Clouddienstleister immer beim (absendenden) Unternehmen liegt, ist eine rechtliche Absicherung erforderlich.

a. Orientierungshilfe

Der Clouddienstleister muss sich zur technisch-organisatorischen Absicherung erklären, diese muss kontrolliert werden und die Daten in der Cloud werden optimaler Weise verschlüsselt. Wenigstens aus der Orientierungshilfe Cloud Computing des Düsseldorfer Kreises aus dem Jahr 2014 (Gremium der deutschen Datenschutzaufsichtsbehörden) werden technisch-organisatorische Maßnahmen vorgestellt, die in rechtlicher und technischer Hinsicht als Standard Beachtung finden sollten.

b. Internationale Cloud-Dienstleister

Im Kontext internationaler Datentransfers müssen Vorgaben zum angemessenen Datenschutzniveau im Empfängerland gewährleistet werden. Hier müssen über Standardvertragsklausel-Verfahren die Transfers abgesichert werden, bei Unternehmen in den USA ergibt sich derzeit eine rechtmäßige Übermittlung, wenn der Datenimporteuer auf der sog. „PrivacyShield-Liste" aufgeführt ist.

9. Bring Your Own Device (BYOD)

Angesichts der Tatsache, dass Mitarbeiter umfangreich eigene mobile Geräte im Unternehmen mitführen, hat sich das Interesse bei Unternehmen entwickelt, die Geräte der Mitarbeiter mit in die Unternehmens-IT-Landschaft einzubinden und die Nutzung auch für dienstliche Zwecke zu erlauben.

a. Sensibilisierung

Hier ist die Errichtung eines Identitätsmanagements genauso erforderlich wie eine Mitarbeiterschulung zum sicheren Umgang, insbesondere wenn Datenpannen stattfinden, die zu Meldepflichten gegenüber Aufsichtsbehörden führen. Bei BYOD sollten keine Cloudservices (Vorsicht bei Apps und webbasierter Software) eingeschalten werden, ebenso wenig Filesharing.

b. Lizenzaudit und Archivierungsregelung

Aus Sicht des Unternehmens und der Geschäftsführung empfiehlt sich eine gezielte Bestandsaufnahme und ein Lizenzaudit, damit nicht Apps für betriebliche Belange genutzt werden, die lizenzrechtlich nur für die private Nutzung freigegeben sind. Im Rahmen des Mobile Device Managements empfehlen sich Archivierungsregelung und Löschberechtigungen von privaten Daten aus der Ferne.

10. Mobile Devices

Unabhängig von dem speziellen Thema „Bring Your Own Device" müssen sämtliche mobilen Geräte aus Sicht des Unternehmens Vorgaben zur Datenspeicherung und Datenübertragung in verschlüsselter Form beachten. Eine automatisierte Datenlöschung muss im Rahmen von Fernwartung möglich sein. Sicherheitsprogramme müssen sich automatisiert aktualisieren und es muss eine Trennung von privaten und betrieblichen Daten möglich sein.

F. KONTROLLE REGELKONFORMEN VERHALTENS ALS BESTANDTEIL DER RISIKOVORSORGE

Die Kontrolle von Mitarbeitern ist seit jeher von den Arbeitsgerichten als zulässig anerkannt, wenn Verhältnismäßigkeitsüberlegungen vorab angestellt wurden und eingehalten werden.

1. Kommunikationsdaten

Kommunikationsdaten dürfen, wenn nur die dienstliche Nutzung für Mitarbeiter gestattet ist, im Rahmen der gesetzlichen Vorgaben uneingeschränkt ausgewertet werden.
Wie bereits erwähnt, ist bei der Nutzungsberechtigung auch für private Zwecke über eine Einwilligungslösung eine entsprechende Kontrolle möglich.

2. Rasterfahndung: Die Suche nach Anomalien

Sowohl bei abstrakten Verdachtsmomenten wie bei konkreten Hinweisen zu Missbrauch sind gewisse Formen von Rasterfahndung im Unternehmen - typischerweise über forensisches Vorgehen - zur Suche nach Auffälligkeiten oder Anomalien zulässig. Dass hier Mitarbeiter-Vertretungsorgane, insbesondere Betriebsräte zu beteiligen sind, versteht sich von selbst. Nach Prüfung der Geeignetheit und Erforderlichkeit eines Datenabgleichs sind Auswertungen unter Gewährleistung des Vieraugenprinzips möglich.

3. Videoüberwachung

Videoüberwachung ist in nicht öffentlich zugänglichen Räumen, z. B. Verwaltungsgebäuden, in denen sich nur Mitarbeiter aufhalten, nach Interessenabwägung sowohl in offener als auch in verdeckter Form zulässig. Letztere heimliche Überwachungsform ist allerdings nur bei konkretem Verdacht einer Straftat oder einer schweren Pflichtverletzung als letztes Mittel statthaft.
In öffentlich zugänglichen Räumen, also Verkaufsbereichen oder öffentlichen Parkplätzen ist eine offene Überwachung grundsätzlich bei Wahrnehmung des Hausrechts zulässig, allerdings muss der Umstand der Beobachtung bekannt gemacht werden. Eine verdeckte Überwachung ist grundsätzlich unzulässig, womit sich viele Fragen derzeit rund um „Dashcams" in Fahrzeugen beschäftigen.

4. Hinweisgebersystem

Eine moderne Form des „Monitorings" von Pflichtverstößen bieten Hinweisgeber-Systeme, in denen „Whistleblower" - geschützt vor dem Vorwurf des Betriebs- und Geschäftsgeheimnisverrats oder arbeitsrechtlicher Pflichtverletzungen - substantiiert Vergehen und Verstöße von Mitarbeitern oder Lieferanten melden.

Da der Hinweisgeber gegebenenfalls anonym bleiben will, erhöht sich die Bereitschaft, regelwidriges Verhalten in entsprechenden Hotlines bekannt zu machen. Für das Unternehmen hat ein Hinweisgebersystem den existentiellen Vorteil, dass der Hinweisgeber hier meldet, statt die Presse oder die Staatsanwaltschaft zu benachrichtigen.

G. ZUSAMMENFASSUNG: KONZEPT DER INFORMATIONSSICHERHEIT ZUR REDUZIERUNG VON IT-HAFTUNGSRISIKEN

Über die strategische, konzeptionelle und operative Vorsorge gegenüber IT-Haftungsrisiken lassen sich Schäden an der IT und durch die IT soweit eingrenzen, dass ein Vorwurf der Verletzung der IT-Risikovorsorge in aller Regel nicht mehr greift. Restrisiken lassen sich üblicherweise über Vermögens- oder Betriebshaftpflichtversicherungen, neuerdings Cyber-Versicherungen, absichern.

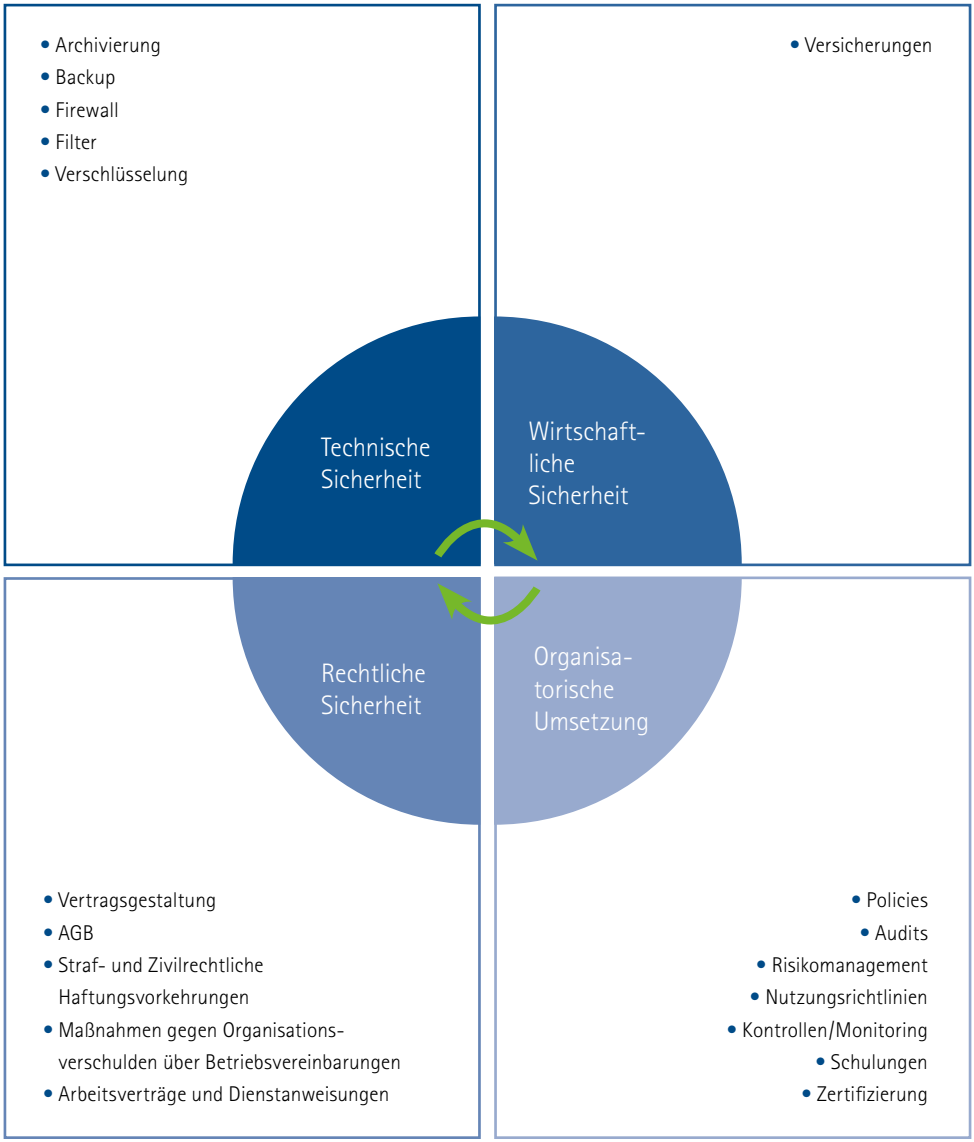
Zusammenfassend lassen sich die Aufgaben der IT-Risikovorsorge wie folgt darstellen:

Konzept der Informationssicherheit

1. Technische Sicherheit ist zu gewährleisten über Archivierung, Backup, Firewall, Filter, Verschlüsselung, Archivierung.
2. Wirtschaftliche Sicherheit über Absicherung der IT-Risiken durch Versicherer.
3. Rechtliche Absicherung erfolgt über Vertragsgestaltung, AGB, straf- und zivilrechtliche Haftungsvorkehrungen, Maßnahmen gegen Organisationsverschulden über Betriebsvereinbarung, Arbeitsvertrag, Dienstanweisungen.
4. Organisatorische Umsetzung erfolgt in Policies, Audits, Risiko-Management, Nutzungsrichtlinien, Kontrollen/Monitoring, Schulungen und Zertifizierung.

Um Haftungsrisiken zu vermeiden, arbeiten Sie sich Schritt für Schritt durch die unterschiedlichen Bereiche, analysieren den jeweiligen Stand im Unternehmen, setzen die notwendigen Maßnahmen um und dokumentieren sie wie gefordert – dann sind Sie rechtlich auf der sicheren Seite!

KONZEPT DER INFORMATIONSSICHERHEIT



Grundlage ist verbindliches IT-Risikomanagement, freigegeben durch die Geschäftsleitung

Checkliste für die Umsetzung der Vorgabe der Europäischen Datenschutz Grundverordnung (GVO)

Rechtsgrundlagen für Datenverarbeitungsvorgänge (Art. 6 GVO) ☐
- Rechtsgrundlagen für Datenverarbeitungsvorgänge analysieren
- Durchsicht der Verfahrensmeldungen, ob Legitimationsprüfung vorhanden ist
- Mitteilung an Abteilungen, dass hier Nachprüfungen gegebenenfalls stattfinden

Informationspflichten (Art. 12–14 GVO) ☐
- Ergänzung von Datenschutzerklärungen oder Verträge mit Datenschutzhinweisen
- Formulierungshinweise an Fachabteilungen zur Einarbeitung

Rechte der Betroffenen (Art. 15–19 GVO, 21 GVO) ☐
- Beschwerdemanagementsystem mit Fristenverwaltung durch festgelegte Abteilung

Recht auf Datenübertragbarkeit (Art. 20 GVO) ☐
- Festlegung Format zur Datenübertragbarkeit von verantwortlicher Stelle zu verantwortlicher Stelle durch IT-Abteilung

Automatisierte Entscheidungen (inkl. Profiling) (Art. 22 GVO) ☐
- Überprüfung nach Profiling-Prozessen und Gewährleistung
- Mindestvorgaben zur Wahrung der Rechte und Freiheiten in relevanten Abteilungen

Umgang mit Daten Verurteilungen/Straftaten (Art. 10 GVO) ☐
- Nachfrage, ob Daten zur Verurteilungen oder Straftaten verarbeitet werden

Implementierung technischer und organisatorischer Maßnahmen und Dokumentation (Art. 24 und 32 GVO) über Compliance Programme DSFA / Bestellung DSB / Audits DS-RL / Training, insbesondere zu:
Implementierung von Datenschutzrichtlinien
- **Einhaltung von Verhaltensregeln**
- **Einhaltung eines genehmigten Zertifizierungsverfahrens**

- Geeignete technische und organisatorische Maßnahmen nach Risikobewertung (Art. 24)
- Sicherheit der Verarbeitung (Art. 32) nach Risikobewertung mit Erklärung der IT-Abteilung oder IT-Dienstleister evtl. über Audit

Dazu die einzelnen dokumentationspflichtigen Bereiche:

Datenschutz durch Technikgestaltung (Art. 25 GVO)
Produktdesign und Zertifizierung, Beachtung Datenschutz „by design" und „by default" (Art. 25) zum Zeitpunkt der Festlegung der Mittel über Bestätigung der IT-Abteilung oder IT-Dienstleister nach Prüfung der Verfahrensmeldungen

Auftragsverarbeiter (Art. 28 GVO)
- Überarbeitung Auftragsdatenverarbeitung-Genehmigungsprozess (Art. 28, 29)
- Service-Prov. Vertrag/Musterklauseln/Pflichten

Verzeichnis Datenverarbeitungstätigkeiten (Art. 30 GVO)
- Verzeichnis der Verarbeitungstätigkeiten über Nachmeldungen in Fachabteilungen (Art. 30) aktualisieren
- Erstellung Verzeichnis über Datenverarbeitungstätigkeiten > Liste als Ergebnis > Update der vorhandenen Dokumentation

Meldung von Verletzungen (Datenpanne) (Art. 32 GVO)
- Überarbeitung „Data Breach" Verfahren (Art. 33, Art. 34) und Ergänzungen im Verfahren IT-Sicherheitsausschuss
- Sicherheitsmaßnahmen/Notfallplan

Datenschutzfolgeabschätzung und Konsultation Aufsicht (Art. 35 GVO)
- Durchführung Datenschutzfolgenabschätzung und Prüfung nach risikobasiertem Ansatz (Art. 35) über Rückmeldung der Fachabteilungen

Internationale Datenübermittlung (Art. 44-47 GVO)
- Gegebenenfalls Nachprüfung internationaler Datentransfers

H. INFORMATIONSQUELLEN

Bitkom-Leitfaden Industrie 4.0 und die neue Rolle der IT

https://www.bitkom.org/Bitkom/Publikationen/Industrie-40-Die-neue-Rolle-der-IT.html

Bitkom-Leitfaden E-Mails und GoBD: 10 Merksätze für die Unternehmenspraxis

https://www.bitkom.org/Bitkom/Publikationen/E-Mails-und-GoBD-10-Merksaetze-fuer-die-Unternehmenspraxis.html

Bitkom-Leitfaden Compliance

https://www.bitkom.org/noindex/Publikationen/2013/Leitfaden/Leitfaden-Compliance/130218-Compliance.pdf

Orientierungshilfe Cloud Computing der Aufsichtsbehörden

https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

BSI Grundschutz Datenschutz

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html

DIE AUTOREN:

Wolfgang A. Schmid

Partner der Kanzlei JuS Rechtsanwälte in Augsburg, Rechtsanwalt, Fachanwalt IT-Recht, beschäftigt sich seit vielen Jahren mit Vertragsgestaltung und Haftungsthemen rund um die IT, seit 2004 externer Datenschutzbeauftragter, Beratung, Ausbildung und Coaching von Datenschutzbeauftragten. Fachspezifische Vorträge / Referententätigkeit zu Haftungsthemen in der IT bundesweit, u. a. seit 2009 bei der Deutschen Anwaltakademie, VKU und TÜV. Zahlreiche Veröffentlichungen zu IT-Themen. Mehr unter www.jus-kanzlei.de

Diane R. Frank Baeza

Rechtsanwältin seit 2008, spezialisiert im Informationstechnologierecht, seit 2010 zertifizierte Datenschutzbeauftragte, seit 2006 Beratung von internationalen Unternehmen im Bereich Compliance und Datenschutz, Ausbildung und Schulung von Datenschutzbeauftragten, fachspezifische Vorträge und Referententätigkeit bundesweit.
Mehr unter www.jus-kanzlei.de

Vera Franz

Rechtsanwältin seit 2010, Fachanwältin IT-Recht, auch spezialisiert im gewerblichen Rechtsschutz und Urheberrecht, Beratung von IT-Unternehmen zu Fragen der Haftung oder Vertragsgestaltung im IT-Umfeld. Mitwirkung bei zahlreichen Veröffentlichungen in IT-Rechtshandbüchern.
Mehr unter www.jus-kanzlei.de

Diese Publikation kann unter
www.digitalisierung-schwaben.de
Nr. 3722304 heruntergeladen werden.
Weitere Informationen zum Thema
IT-Sicherheit finden Sie unter
www.digitalisierung-schwaben.de

Ihre Ansprechpartner:

Anna-Fiora Kilger
Geschäftsfeld Innovation, Umwelt und Energie
Fachbereich Digitalisierung und IT

Telefon: 0821 3162-406
anna.kilger@schwaben.ihk.de

Stefan Schimpfle
aitiRaum e. V.
Geschäftsführer

Telefon: 0821 450433-111
s.schimpfle@aitiRaum.de

Herausgeber:
IHK Schwaben
Stettenstraße 1+3
86150 Augsburg

info@schwaben.ihk.de
www.schwaben.ihk.de

Redaktion:
aitiRaum e. V.
Andrea Henkel

Bildnachweis:
Titel: Fotolia
Innenteil: iStock, Shutterstock

Gestaltung:
°SPRINGFLUT GmbH
www.springflut.com

Stand: Mai 2017

IHK Schwaben
Arbeit für Schwaben