Mittelstand 4.0
Kompetenzzentrum
Planen und Bauen

KOMPAKT

Was bedeutet IT-Compliance?

Eine Handreichung für Handwerksbetriebe

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Was bedeutet IT-Compliance?

„IT-Compliance beschreibt in der Unternehmensführung die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft.“ [1]

Legalitätspflicht

Die Notwendigkeit, sich mit dem Thema IT-Compliance zu befassen, folgt aus der Verpflichtung der Geschäftsleitung, für den rechtskonformen Ablauf aller betrieblichen Vorgänge Sorge zu tragen. Für den häufigen Fall, dass der Betrieb in der Rechtsform der GmbH organisiert ist, obliegt die Pflicht dem Geschäftsführer. Dieser hat gem. § 43 GmbHG die Geschäfte mit der Sorgfalt eines ordentlichen Geschäftsmannes vorzunehmen. Verletzt er geltendes Recht und entsteht der Gesellschaft dadurch ein Schaden, haftet er persönlich.

Kommunizieren

Smartphone und E-Mail werden ganz selbstverständlich zur Kommunikation mit Kunden und Mitarbeitern verwendet. Ist die private Nutzung zugelassen, ist ein Zugriff auf Gerät und Postfächer durch den Betrieb nicht ohne weiteres möglich. Es bedarf der Zustimmung des Mitarbeiters und einer betrieblichen Regelung. Werden geschäftliche Erklärungen per E-Mail übermittelt, handelt es sich um Geschäftsbriefe. Für sie gelten die Bestimmungen, die auch für Papier gelten, also Pflichtangaben und Aufbewahrung sind zu organisieren.

Präsentieren

Viele Betriebe betreiben eine eigene Homepage. Sie dient vorwiegend der Kundenansprache. Das Thema „Datenschutzerklärung“ fällt dabei nur zu oft unter den Tisch. Dies gilt selbst dann, wenn die Website durch eine Agentur gestaltet und betreut wird. Ferner werden zur Gestaltung Bilder und Texte sowie Videosequenzen verwendet, deren Herkunft bisweilen nicht klar ist. Beide Felder Datenschutz und Urheberrecht sind Einfallstore für Abmahner, deren Geschäftsmodell das Ausnutzen von Fehlern anderer ist.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

Archivieren

Üblicherweise werden Dokumente, die mit dem PC erstellt wurden, auf der Festplatte des Geräts abgelegt. Dies geschieht im Vertrauen darauf, dass das Gerät nicht ausfällt. Wenn es dann doch zum Ausfall kommt, so wird die Hoffnung auf schnellen Ersatz und eine kurze Unterbrechung häufig enttäuscht. Werden solche Fälle jedoch bedacht, lassen sich zielgerichtet Vorkehrungen treffen. Dies betrifft nicht nur die Datensicherung, sondern auch Probleme bei der Stromversorgung und die Entsorgung nicht mehr benötigter Daten.

Dokumentieren

Europäische Datenschutz-Grundverordnung (DS-GVO) und die von dem Bundesfinanzministerium herausgegebenen Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zu Datenzugriff (GoBD) sehen jeweils vor, dass der Einsatz von IT-Werkzeugen in einer Dokumentation festgehalten wird. Beide Regelwerke machen Vorgaben zum Mindestinhalt. Sie weisen in den Bereichen Datensicherheit eine Schnittmenge auf. Dies ermöglicht Synergien.

Überwachen

Das Einhalten der gesetzlichen Bestimmungen erfordert Überwachung. Die Geschäftsleitung muss die Betriebsabläufe im Blick haben. Dabei dürfen ihr aber auch technische Neuerungen nicht entgehen. Wie im eigenen Gewerk der Wandel der anzuwendenden Arbeitstechnik und Maschinen, muss von Zeit zu Zeit der Fortschritt in der IT betrachtet werden. Darüber hinaus dürfen der Geschäftsleitung rechtliche Neuerungen nicht nur im Bereich technischer, sondern auch IT-rechtlicher Natur nicht entgehen. Fortbildung ist Pflicht!

Einspielen

Wird im Zuge der Überwachung ein Änderungsbedarf erkannt, muss dieser im Betrieb umgesetzt werden. Änderungsbedarf kann sich mit Blick auf das Geschäftsmodell ergeben, wenn etwa Normen ein Angebot gegenüber Kunden wie bisher nicht mehr zulassen. Er kann aber auch aus technischen Neuerungen folgen. Veraltete Technik kann Unsicherheiten bergen, die von dem Betrieb nicht mehr akzeptiert werden können. Auf den Weg sind die Mitarbeiter mitzunehmen. Ihr Verhalten bestimmt die Compliance.

[1] Definition nach wikipedia: https://de.wikipedia.org/wiki/IT-Compliance (abgerufen am 12.02.2018). Artikel Lizenziert unter CC-BY-SA 3.0 unported, abrufbar unter: https://de.wikipedia.org/wiki/Wikipedia:Lizenzbestimmungen_Creative_Commons_Attribution-ShareAlike_3.0_Unported (abgerufen am 12.02.2018).

Checkliste – Zehn-Punkte-Plan für mehr IT-Compliance

Lfd.Nr.	Maßnahme	Handlungsbedarf			Informationsbedarf		
		Gering	Mittel	Hoch	Gering	Mittel	Hoch
1	IT-Werkzeuge im Unternehmen sind erfasst, d.h. Hardware wie z.B. Server, Router, Switches, PC, Laptops, Tablets, Smartphones und Software wie z.B. Betriebssysteme, Office-Pakete, Branchensoftware etc. sind aufgelistet, ggf. ist ihre Einbindung in betriebliches Netzwerk organisatorisch und räumlich aufgezeichnet.	○	○	○	○	○	○
2	Die Anforderungen an den betrieblichen Datenschutz sind ermittelt, die Unterrichtung der Mitarbeiter im Umgang mit Kunden- und Mitarbeiterdaten ist durchgeführt und dokumentiert.	○	○	○	○	○	○
3	Die Homepage ist auf ein korrektes Impressum und eine zutreffende Datenschutzerklärung kontrolliert und juristisch überprüft, alle Pflichtangaben sind vorhanden, etwa erforderliche Einwilligungen sind eingeholt und ihr Vorliegen wird ordnungsgemäß dokumentiert, ggf. ist mit dem IT-Dienstleister die Protokollierung abgestimmt und eingerichtet.	○	○	○	○	○	○
4	Die Anforderungen an die steuerrechtliche Dokumentation von Geschäftsvorfällen, insbesondere solche aus den GoBD sind ermittelt und Maßnahmen zu ihrer Einhaltung bestimmt und umgesetzt.	○	○	○	○	○	○
5	Benutzungsregeln für IT-Werkzeuge sind erstellt, d.h. es ist festgelegt, wer welches IT-Werkzeug in welcher Weise benutzt; es ist festgelegt, wie im Falle einer unvorhergesehenen Abwesenheit eines Mitarbeiters mit Geräten und Nutzerkonten z.B. für E-Mail verfahren wird.	○	○	○	○	○	○
6	Die Verfügbarkeit von IT-Werkzeugen und der betrieblich erforderlichen Daten ist durch ein Backup-System und eine unterbrechungsfreie Stromversorgung ggf. bei dem IT-Dienstleister und im Betrieb selbst sichergestellt; es wird gewährleistet, dass nicht mehr benötigte Daten anforderungsgerecht gelöscht bzw. entsorgt werden.	○	○	○	○	○	○
7	Die Überwachung der Einhaltung betrieblicher Anweisungen sowie von technischen und rechtlichen Neuerungen ist gewährleistet; ein internes Kontrollsystem ist installiert und eingerichtet.	○	○	○	○	○	○
8	Die Dokumentation der Leistungsbeziehungen und des IT-Einsatzes sind entsprechend den Anforderungen, insbesondere denjenigen aus DS-GVO und GoBD erstellt und kann auf Anforderung vorgelegt werden.	○	○	○	○	○	○
9	Der IT-Compliance-Prozess ist initiiert, in Gang gesetzt und wird aufrechterhalten; d.h. es ist sichergestellt, dass Handlungsbedarf identifiziert und Anforderungen zeitnah in den Betriebsablauf eingespielt werden können.	○	○	○	○	○	○
10	Fördermöglichkeiten für Beratungsleistungen sind ermittelt, ein Termin mit einem Berater für eine individuelle IT-Compliance-Beratung ist vereinbart, die Beantragung von Fördermitteln ist vorbereitet.	○	○	○	○	○	○

Es wird empfohlen, fachkundigen Rat ggf. bei einer zur Rechtsberatung zugelassenen Stelle wie z.B. einem Rechtsanwalt einzuholen.

Impressum: eBusiness-KompetenzZentrum gUG (haftungsbeschränkt), Mittelstand 4.0-Kompetenzzentrum Planen und Bauen, Teilzentrum Mitte, Europaallee 10, 67657 Kaiserslautern, Geschäftsführer: Michael Heil
Redaktion: Ass. iur. Michael Weller, Senior-Berater IT-Compliance, E-Mail: m.weller@ebusiness-kompetenzzentrum.de, Telefon: 0631/205601-801; Druck: Dummy-Druck 2018. Bilder: www.pixabay.com, verw. u. d. CC0 Public Domain Dedication https://creativecommons.org/publicdomain/zero/1.0/deed.de.