Mittelstand 4.0
Kompetenzzentrum
Rostock

DATENSCHUTZ & IT-SICHERHEIT IM HOTELBETRIEB

Intelligente digitale Lösungen im Tourismus

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

„Für Unternehmer muss IT-Sicherheit Bestandteil der Digitalisierung sein.“

Mittelstandspräsident Prof. Dr. h.c. Mario Ohoven

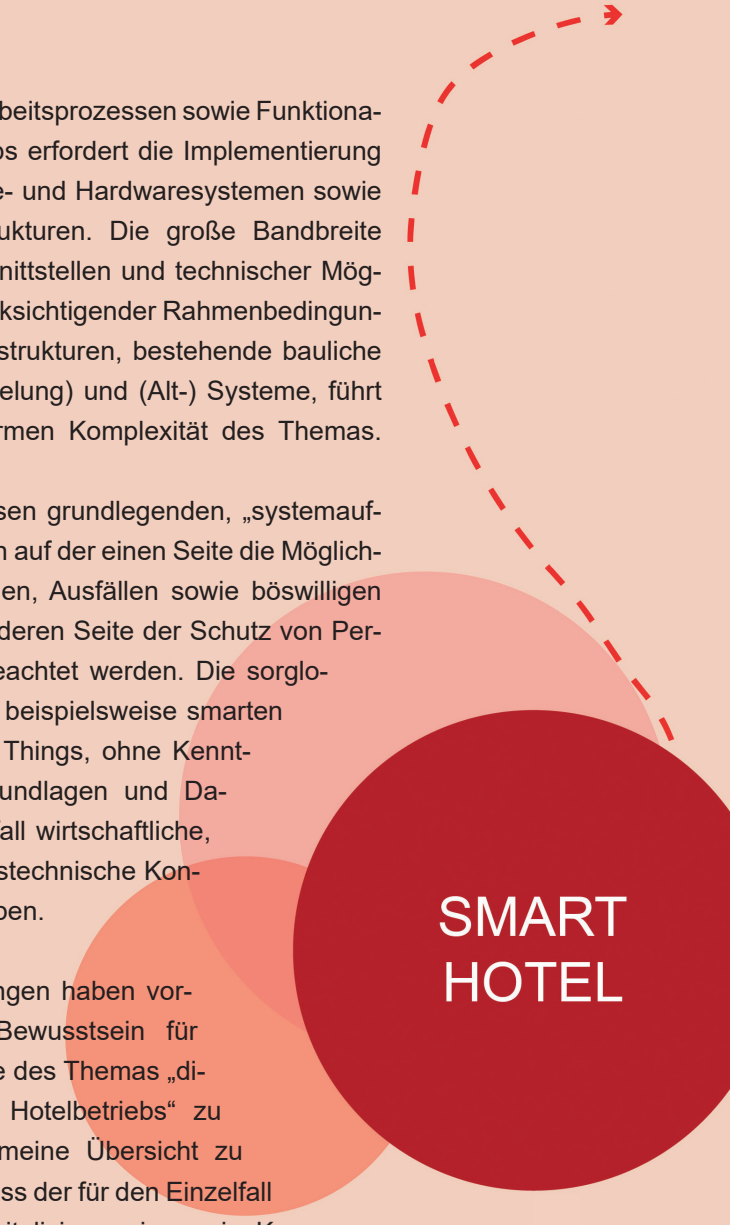
1 Handy am Strand

INHALT

EINFÜHRUNG

Die Digitalisierung von Arbeitsprozessen sowie Funktionalitäten eines Hotelbetriebs erfordert die Implementierung von geeigneten Software- und Hardwaresystemen sowie geeigneten Netzwerkstrukturen. Die große Bandbreite möglicher Systeme, Schnittstellen und technischer Möglichkeiten sowie zu berücksichtigender Rahmenbedingungen wie öffentliche Infrastrukturen, bestehende bauliche Strukturen (z. B. Verkabelung) und (Alt-) Systeme, führt allerdings zu einer enormen Komplexität des Themas.

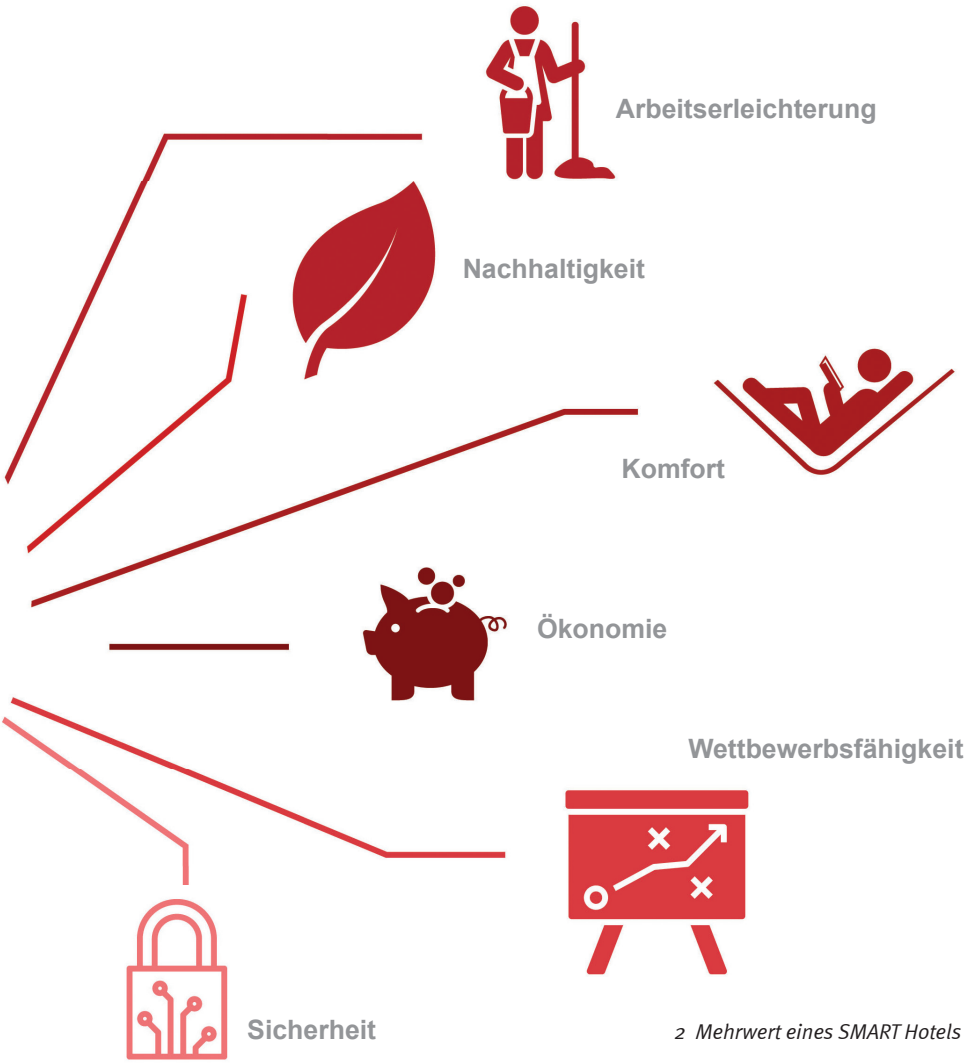
Zudem muss neben diesen grundlegenden, „systemaufbauenden“ Überlegungen auf der einen Seite die Möglichkeit von Fehlern, Schäden, Ausfällen sowie böswilligen Angriffen und auf der anderen Seite der Schutz von Personen und Systemen beachtet werden. Die sorglose Implementierung von beispielsweise smarten Geräten des Internet of Things, ohne Kenntnis der technischen Grundlagen und Datenflüsse kann im Ernstfall wirtschaftliche, rechtliche und sicherheitstechnische Konsequenzen zur Folge haben.



Die folgenden Ausführungen haben vorrangig das Ziel das Bewusstsein für verschiedene Teilaspekte des Themas „digitale Strukturen eines Hotelbetriebs“ zu wecken und eine allgemeine Übersicht zu geben. Grundsätzlich muss der für den Einzelfall sinnvollste Weg einer Digitalisierung immer im Kontext des jeweiligen Unternehmens angegangen werden.

Dieses Themenheft behandelt einen Teilbereich eines SMARTEN Hotels. Mehr Informationen zur Digitalisierung weiterer Bereiche wie Öffentlichkeitsarbeit, Management, Gebäude sowie Mobilität finden Sie in dem „Leitfaden SMART Hotel“. Dieser soll Hoteliers durch ein 3-Stufen-System (SMART, SMART plus und all SMART) dabei unterstützen, den Stand der Digitalisierung des eigenen Hotels einschätzen zu können, die Potentiale neuer Technologien kennenzulernen und einen Überblick über den Markt sowie dessen Möglichkeiten zu bekommen – individuell abgestimmt auf das eigene Hotelkonzept.

>> Hier gelangen Sie zum Leitfaden SMART Hotel



2 Mehrwert eines SMART Hotels

STRATEGIE EINER DIGITALEN TRANSFORMATION

Die Implementierung digitaler Strukturen hängt von verschiedenen Faktoren ab, wie der strukturellen Ausgangssituation und dem finanziellen Rahmen des Unternehmens. Zudem muss bei den Verantwortlichen ein gewisses Maß an rechtlicher und technischer Übersicht vorliegen, damit die richtigen Fragen gestellt, Lösungen bewertet und geeignete Entscheidungen getroffen werden können.

Grundsätzlich sind zur Ausgestaltung digitaler Strukturen verschiedenste Lösungsansätze denkbar. Von der Optimierung einzelner, isolierter Prozesse bis hin zu vollvernetzten Kommunikations- und Analysestrukturen ist einiges möglich.

Für jeden Geschäftsprozess und jede technische Struktur eines Unternehmens existieren auf dem Markt unterschiedlichste Angebote verschiedener Hersteller mit verschiedensten technischen Realisierungen und ggf. Serviceunterstützung. Hier gilt es zu entscheiden, welche Lösung für das eigene Unternehmen sinnvoll ist. Eine schrittweise und gleichzeitig agile Herangehensweise, die das Unternehmen als Ganzes sieht bzw. strukturelle Zusammenhänge berücksichtigt, sollte hierbei leitend sein.

Die rechtzeitige Einbindung bzw. Konsultation von Experten sowohl im rechtlichen als auch technischen Bereich ist für das Gelingen eines sinnvollen digitalen Wandels des eigenen Unternehmens auf jeden Fall ratsam.
Im Folgenden werden grundsätzliche Schritte skizziert.

1. Schritt – Analyse des Ist-Zustands

Eine smarte Infrastruktur sollte immer in Hinblick auf das Erreichen konkreter wirtschaftlicher und nachhaltiger Ziele geplant und umgesetzt werden. Um diese Ziele definieren zu können, ist es notwendig, zunächst eine grundlegende Bestandsaufnahme durchzuführen. Die folgenden Themenbereiche sollten betrachtet werden:

- Technische und bauliche Strukturen: Welche baulichen, informationstechnologischen und anlagetechnischen Strukturen liegen bereits vor?
- Schwachstellen: Sind ineffiziente Arbeitsabläufe, hohe Betriebskosten in bestimmten Bereichen oder Kritik von Gästen, Mitarbeitern oder Lieferanten bekannt?
- Hotelprofil: Was sind die Stärken und Schwächen des Hotels? Welche Anforderungen und Erwartungen haben die Gäste? Lohnt sich in Hinblick auf das konkrete Hotelprofil die Etablierung als SMART Hotel?
- Fachwissen: Welches fachliche Wissen liegt vor bzw. wird benötigt?

2. Schritt – Erstellung eines Konzepts

Basierend auf dem Ist-Zustand des Hotels können mögliche Geschäftsprozesse und Anwendungsfälle ermittelt werden, die von einem Einsatz smarter Technologien profitieren. Für den konkreten Anwendungsfall werden anschließend mögliche Lösungen sowie zugehörige technischen Umsetzungen erarbeitet. Hierbei sollten die folgenden Aspekte berücksichtigt werden:

- Integration in die bestehenden Systemstrukturen und / oder Geschäftssysteme
- Verwendung zukunftssicherer, aktualisierbarer und dem Bedarf entsprechend skalierbarer Technologien
- Kompatibilität verschiedener Geräte unterschiedlicher Hersteller; Transparenz der Kommunikation und ggf. Cloudinfrastrukturen
- Kosten-Nutzen-Bewertung
- Datenverarbeitung (Art, Umfang, Wege und Ort der Speicherung)
- Sicherheits- und Risikobewertung

3. Schritt – Inbetriebnahme

Bevor das System in Betrieb geht, sollte der fehlerfreie Einsatz getestet werden und ein Sicherheitskonzept für den Fall des Ausfalls vorliegen. Zudem müssen die rechtlichen Anforderungen erfüllt sein. Das Hotelpersonal muss hierauf geschult werden und ggf. auf den Notfall vorbereitet sein.

4. Schritt – Fortlaufender Betrieb

Im Betrieb einer digitalen Infrastruktur muss eine fortlaufende Systembetreuung und -überwachung erfolgen. Hierzu gehört das Einspielen von Sicherheitspatches und Updates bzw. Upgrades wie auch ein fortlaufendes Änderungsmanagement, um den Stand der Technik zu erhalten.

4 Sicherheit im Internet

GEFAHREN

Bei der Planung und Implementierung der Strukturen und Systeme gilt es sich bewusst zu machen, welchen Gefahren eine digitale Infrastruktur ausgesetzt ist. Dies ist notwendig zum einen aus Sicht des Schutzes der fortlaufenden Geschäftsprozesse und Vermögenswerte des Unternehmens und zum anderen um gesetzlichen Bestimmungen nachzukommen. Den potentiellen Bedrohungen sollte mit entsprechenden technischen und organisatorischen Maßnahmen begegnet werden. Liegen hier Mängel vor, steigt das Risiko eines Schadens. Im Folgenden werden vier grundlegende Gefahrenbereiche beschrieben.

► Technisches Versagen / Systemausfall

Zu nennen sind hier die Störungen der Stromversorgung, der Kommunikations- und Versorgungsnetze oder der Ausfall von Dienstleistern. Problematisch sind auch Altsysteme (Fehlen der Ersatzteile, proprietäre Strukturen).

► Menschliche Fehlhandlungen

Hier gehören z. B. das Öffnen der unbekannten E-Mail-Anhänge, Stecken gefundener USB-Sticks in interne Computer oder Schäden durch fehlerhafte Bedienung/ Nutzung eines Systems (Datenverlust, Systemausfall).

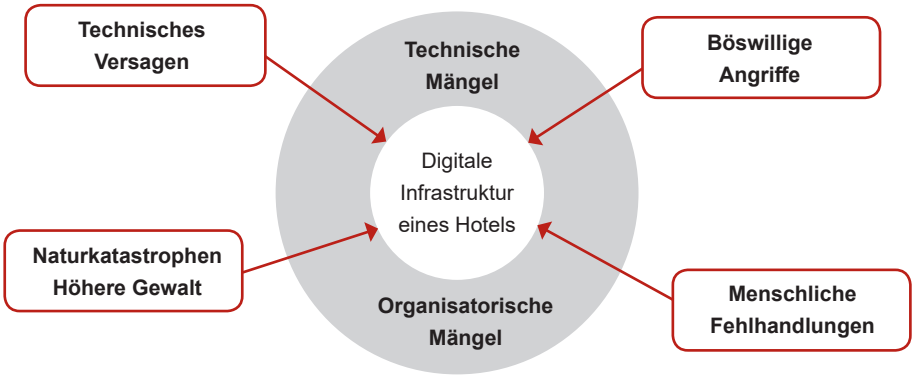
► Böswillige Angriffe

Angreifer nutzen Sicherheitslücken und Schwachstellen in Computersystemen und im Internet aus. Beispiel von böswilligen Angriffen sind Social Engineering Attacken, bei welchen versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren (Vgl. Bundesamts für Sicherheit in der Informationstechnik (BSI); Zugriff 08/2019).

>> Eine Sammlung verschiedener Vorfälle im Hotelgewerbe zeigen beispielsweise die folgenden Websites (10/2019):
► http://www.hotelnews-now.com/Articles/ 50937/ Timeline-The-growing-number-of-hotel-data-breaches
► www.datenschutzticker.de

► Organisatorische und technische Mängel

Zu den organisatorischen Mängel gehören beispielsweise Regelungen bei Personalausfall oder einem eintretenden Notfall, aber auch fehlende Ansprechpartner/innen oder fehlende Ausweichmöglichkeiten im Falle eines Ausfalls eines Dienstleisters.
Beispiele für technische Mängel sind Fehler in Software, Fehlkonfigurationen oder auch technische Schwachstellen, die durch ein fehlendes oder nicht ausreichendes Änderungs- bzw. Wartungsmanagement entstehen.



5 Bedrohungslage einer digitalen Infrastruktur eines Hotels

6 DSGVO

RECHTLICHE UND SICHERHEITSTECHNISCHE ANFORDERUNGEN

Ein Hotelbetrieb muss zahlreichen Vorschriften aus unterschiedlichen Rechtgebieten beachten. Dieser Abschnitt thematisiert die rechtlichen Anforderungen, die in Hinblick auf den Betrieb einer digitalen Infrastruktur eines Hotelbetriebs beachtet werden müssen. Hier gehören vor allem das Datenschutzrecht, aber auch weitere Gesetze. Welche Gesetze allerdings für eine konkrete Fallkonstellation anwendbar sind, hängt vom Einzelfall ab.

Datenschutz

In Hinblick auf den Betrieb einer digitalen Hotelinfrastruktur ist vor allem das Datenschutzrecht eine wichtige rechtliche Vorschrift. Das maßgebliche Gesetz hierzu ist die europäische Datenschutzgrundverordnung (DSGVO), auf nationaler Ebene spezifizieren Bestimmungen des Bundesdatenschutzgesetzes (BDSG) verschieden Bereiche der DSGVO. Das grundsätzliche Anliegen des Datenschutzes ist es, die Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten – zu schützen.

Die grundlegenden Gedanken einer rechtskonformen Datenverarbeitung können mit den folgenden Schlagworten charakterisiert werden:

>> Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

► Rechtmäßigkeit

Rechtmäßigkeit bedeutet, dass eine Rechtsgrundlage vorliegen muss, die eine Verarbeitung personenbezogener Daten erlaubt.

► Verarbeitung nach Treu und Glauben

Treu und Glaube bedeutet beispielsweise, dass die betroffene Person davon ausgehen kann, dass ihre personenbezogenen Daten ordentlich und rechtskonform verarbeitet werden sowie deren Schutz gewährleistet wird.

► Transparenz

Der leitende Gedanke der Transparenz bedeutet zum einen, dass die betroffene Person weiß, wie, von wem und warum welche Daten verarbeitet werden und entsprechend ihre Rechte geltend machen kann („Intervenierbarkeit“), zum anderen aber auch, dass die Datenverarbeitung verantwortlichen Stellen transparent im Rahmen der Rechenschaftspflichten dargelegt wird.

Die DSGVO definiert weiterhin konkrete Eigenschaften, die eine rechtskonforme Verarbeitung (Datensparsamkeit, Zweckbindung) bzw. datenverarbeitende informationstechnische Systeme (Vertraulichkeit, Integrität, Verfügbarkeit) auszeichnen. Die datenschutzkonforme Datenverarbeitung muss durch geeignete technische und organisatorische Maßnahmen (TOM) gewährleistet werden.

Datenschutzkonzept

Im Datenschutzrecht explizit festgeschrieben ist der Gedanke der Rechenschaftspflicht, wonach der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO vor allem bei den Aufsichtsbehörden nachweisen können muss (Art. 5 Abs. 2). Dokumentations- und Nachweispflichten ergeben sich hierbei u.a. aus den Artikeln 24, 28, 30, 33 der DSGVO. Konkret müssen die folgenden Unterlagen vorliegen:

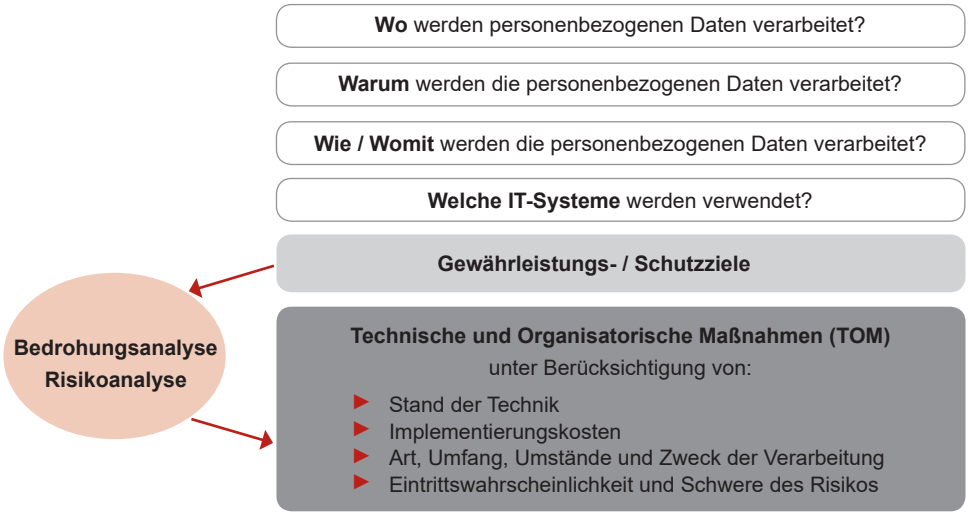
- Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen nach Art. 30 Abs. 1 DSGVO. Hinsichtlich der geforderten Dokumentation von technischen und organisatorischen Maßnahmen (TOM) im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten kann auf das IT-Sicherheitskonzept verwiesen werden.
- Schriftliche Verpflichtungserklärungen der Mitarbeiter, die im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten, auf das Datengeheimnis (Art. 29 DSGVO i.V.m. Artikel 32 Abs. 4 DSGVO). Administratoren sollten in Hinblick auf die unterschiedlichen Ansichten der Landesdatenschutzbeauftragten und der Rechtsprechung sicherheitshalber auch auf § 88 TKG verpflichtet werden.
- Regelungen entsprechend Art. 28 DSGVO bei Auftragsverarbeitung: Schriftliche Auftragsverarbeitungs-Vereinbarung
- Dokumentation/ Meldung von Datenschutzvorfällen an die Aufsichtsbehörde

Zudem muss der Verantwortliche seinen Informations- und Transparenzpflichten gegenüber der betroffenen Person durch geeignete Aufklärung nachkommen. Die Generalklausel hierzu ist Art. 12 DSGVO. Entsprechend müssen beispielsweise Gäste, Interessenten oder Mitarbeiter darüber informiert werden, in welchem Rahmen eine Datenverarbeitung stattfindet und welche Rechte sie haben. Hierunter fällt neben dem Hinweis zum Einsatz von Cookies auf Webseiten, auch beispielsweise die Hinweisbeschilderung zum Einsatz von Videoüberwachung oder das Aufzeichnen der Arbeitsleistung von Mitarbeitern.

Datenschutzbeauftragter und Informationsquellen

Die Aufgabe eines Datenschutzbeauftragten ist es, eine Institution hinsichtlich datenschutzrechtlicher Anforderungen zu beraten sowie die ordnungsgemäße Durchführung zu überprüfen. Die Frage, ob für ein Hotel eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, kann nicht allgemeingültig beantwortet werden. Beschäftigt das Hotel regelmäßig mind. 10 Personen (mit Umsetzung des 2. DSAnpUG wird die Zahl auf 20 angehoben) mit der automatisierten Verarbeitung personenbezogener Daten, ist nach § 38 Abs. 1 BDSG die Bestellung eines Datenschutzbeauftragten notwendig. Aber auch wenn diese Zahl nicht erreicht wird, kann aufgrund der mitunter sensiblen personenbezogenen Daten, die in einem Hotel verarbeitet werden, eine Pflicht bestehen. Im jeden Fall ist eine datenschutzrechtliche Beratung sicherlich anzuraten.

>> Datenschutzgrundverordnung online (7/2020): ► https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE



7 Datenschutzrechtliche Bewertung von Verarbeitungstätigkeiten

8 IT-Sicherheit und Vorschriften

SONSTIGE RELEVANTE VORSCHRIFTEN

Neben den datenschutzrechtlichen Vorschriften sind eine Vielzahl weiterer Rechtsvorschriften durch die Digitalisierung eines Hotels betroffen. Aufgrund der Vielzahl der, je nach Einzelfall betroffenen, gesetzlichen Regelungen kann an dieser Stelle nur ein kurzer Überblick über die wichtigsten Gesetze und Regelungen gegeben werden. Jeder Hotelbetrieb sollte sich grundsätzlich juristisch beraten lassen.

► Bürgerliches Gesetzbuch (BGB)

Da die Digitalisierung neue Gefahren für die durch das BGB geschützten Rechtsgüter der Gäste schafft, wird das BGB v. a. im Bereich des Deliktsrechts wichtig – zu denken ist etwa an einen Diebstahl von Kreditkartendaten oder blockierte vernetzte Türschlösser und die hieraus folgenden Schadensersatzansprüche der Gäste.

Auch die Haftung für illegale Aktivitäten der Gäste unter Benutzung des angebotenen WLAN-Zugangs ist weiterhin zu beachten. Teilweise können diese Folgen über allgemeine Geschäftsbedingungen (AGB) eingegrenzt werden, wobei hier allerdings dem gewerblichen Verwender von AGBs enge Grenzen gesetzt werden.

► Handelsgesetzbuch (HGB)

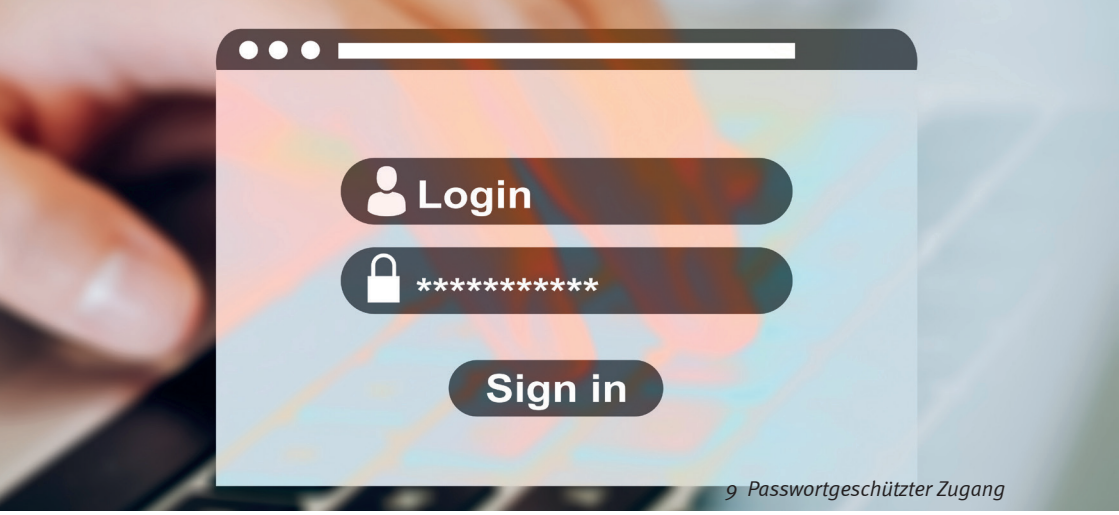
Das für Hotels als Gewerbebetriebe anwendbare HGB schreibt dem/der Kaufmann/frau unabhängig von der konkreten Gesellschaftsform v. a. strenge Buchführungspflichten vor. Bei einer Digitalisierung des Buchungs- und Abrechnungssystems eines Hotels werden diese Vorschriften durch die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) präzisiert (Vgl. Bundesministerium der Finanzen; Zugriff 08/2019). Spezielle Systemanforderungen werden hier nicht gestellt, sondern durch einen Vergleich mit der analogen Buchführung festgestellt.

► Telemediengesetz (TMG)

Das TMG stellt Regelungen für alle Hotels auf, die eine Website betreiben (inklusive sämtlicher möglicher Angebote wie Blogs, Online-Gästebücher usw.) wie und / oder den Gästen über das hoteleigene WLAN den Zugang zum Internet ermöglichen. So muss etwa die Homepage Angaben zu Name, Anschrift, Rechtsform, Vertretungsberechtigten, Handelsregistereintrag samt Registrierungsnummer und die Möglichkeiten einer Kontaktaufnahme enthalten. Auch werden strenge Anforderungen bzgl. der Erhebung und Verwertung personenbezogener Daten aufgestellt.

► Payment Card Industry Data Security Standard (PCI DSS)

Bei dem PCI DSS (Vgl. Security Standards Council; Zugriff 08/2019) handelt es sich nicht um ein Gesetz, als vielmehr um allgemeine Geschäftsbedingungen, also zivilrechtliche Regelungen, mit denen die Anbieter von Zahlungskarten Gewerbetreibenden, die ihren Kunden die Option einer Kartenzahlung anbieten, bestimmte Sicherheitsanforderungen an deren Bezahlsysteme vorgeben. Das Ziel ist die Verbesserung der Sicherheit von Karteninhaberdaten und die weltweite Vereinheitlichung und Vereinfachung von Datensicherheitsmaßnahmen sowie Online-Kreditkartenzahlungen.



9 *Passwortgeschützter Zugang*

IT-SICHERHEITSKONZEPT

Die Bedrohungslage, der eine digitale Hotelinfrastruktur ausgesetzt ist, ist sehr vielfältig und hängt vor allem davon ab, welche Systeme und Techniken verwendet werden. Um den datenschutzrechtlichen und sicherheitstechnischen Anforderungen gerecht zu werden, sollte ein strukturiertes und für Dritte nachvollziehbares IT-Sicherheitskonzept vorliegen. Im Folgenden werden die grundsätzlichen Schritte, die bei der Erstellung eines IT-Sicherheitskonzeptes bedacht werden sollten, vereinfacht zusammengefasst.

- Struktur- und Schutzbedarfsanalyse: Bestimmung der zu schützenden Systeme / Objekte sowie der zu gewährleistenden Schutzziele
- Risikoanalyse: Analyse der möglichen Gefahren (Bedrohungsanalyse) und Schadenszenarien sowie deren Eintrittswahrscheinlichkeit
- Modellierung der Sicherheitsstrategie:
  - Entwicklung von TOM (Technische und Organisatorische Maßnahmen), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
  - Planung von Maßnahmen bei Schadenseintritt
  - Planung der Systempflege und Dokumentation

In Hinblick auf die finanziellen und personellen Gegebenheiten kleiner und mittlerer Unternehmen gilt es eine ausgewogene und mitunter pragmatische Mischung aus bezahlbaren Verfahren und höchstmöglicher Absicherung zu finden. Das Ziel sollte es sein, ein möglichst effizientes und übersichtliches Vorgehen zu etablieren, das zum einen ermöglicht den Anforderungen und Auflagen des Datenschutzrechts transparent nachzukommen und zum anderen den Überblick über die eigene IT zu behalten und diese fortlaufend sicher zu betreiben. Konkret sollten die folgenden Unterlagen vorliegen:

- Beschreibung der IT-Strukturen und Systeme
- Beschreibung der TOM
- Wartungsplan und Änderungsmanagement
- Notfallplan (Verantwortlichkeiten, Alarmierungsketten/ Kommunikationsregelungen, Kontaktinformationen, technische Anweisungen und Maßnahmenlisten)
- IT-Richtlinien, Benutzerrichtlinien, Arbeitsanweisungen
- Nachweis der Schulung der Mitarbeiter

>> Im Bereich der IT-Sicherheit existieren verschiedene standardisierte Herangehensweisen zur Erstellung eines IT-Sicherheitskonzepts. Eine Übersicht hierzu liefert die Webseite des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom e.V.): www.kompass-sicherheitsstandards.de

Sind Sie bereits kompromittiert? Haben Sie dies überprüft? Kennen Sie Ihre Bedrohungslage bzw. Schwachstellen?

Wie gut sind Ihre TOM zur Absicherung Ihres Unternehmens? Testen Sie wie ein echter Hacker? Lohnt sich ggf. eine Versicherung?

Wissen Sie, wo sich Ihre Daten befinden und wer Zugriff darauf hat? Vertrauen Sie blind der Cloud oder wissen Sie über die technischen Hintergründe Bescheid?

Was würden Sie tun, wenn Sie bemerken, dass Sie angegriffen wurden? Sind Ihre Notfallpläne geeignet rechtlichen Anforderungen nachzukommen?

Wie schneiden Sie gegenüber anderen Betrieben ab? Was ist Ihr RoI (Return on Investment)? Wie vergleichen Sie sich zu Best Practice?

10 IT- und Datensicherheit in der Hotellerie – fünf wichtige Fragen, die Sie sich stellen sollten

11 Beispiel WLAN-Router

Beispiel WLAN

Ein zuverlässiges und sicheres Wireless Local Area Network (WLAN), das Gästen einen kabellosen Internetzugang bereitstellt, ist eine Grundvoraussetzung einer smarten Infrastruktur eines Hotels. Heutzutage wird grundsätzlich erwartet, dass ein kostenfreier, schneller und im gesamten Hotelbereich gleichmäßig verfügbarer WLAN-Zugang vorhanden ist.

Infrastruktur

Hier sind zum einen strukturelle Fragestellungen zu klären, wie z. B. die mögliche Anzahl der Gäste (die gleichzeitig eine stabile und ausreichende Bandbreite erwarten), den zu versorgenden Bereich des Gebäudes / der Anlage (Reichweite) sowie die vorhandenen technischen Strukturen (verlegte Kabel, eingesetzte Verwaltungssysteme usw.) bzw. die eventuell existierenden Schwachstellen der im Einsatz befindlichen WLAN-Lösung. Neben diesen internen Überlegungen muss natürlich der Standort des Hotels und die zugehörige öffentliche Infrastruktur gesehen werden.

>> WEP / WPA / WPA2 / WPA3-Verschlüsselung sind Verschlüsselungsprotokolle für WLAN. WEP (Wired Equivalent Privacy) ist das älteste Verfahren und sollte nicht mehr verwendet werden, da sie keinen ausreichenden Schutz bietet. WPA (Wi-Fi Protected Access) sind Nachfolger.
Unter einem Pre-Shared Key (PSK) versteht man in der Kryptographie einen geheimen Schlüssel für ein symmetrisches Verschlüsselungsverfahren, der beiden Kommunikationspartner bereits bekannt ist (Vgl. IT-Administrator; Zugriff 08/2019).

Hinsichtlich der Reichweite eines WLAN muss bedacht werden, dass mit zunehmender Entfernung vom Router das Signal schwächer und die Verbindung langsamer und instabiler wird – das Signal muss daher technisch „weitergetragen“ werden. Grundsätzlich kann das Signal über Festnetzleitungen oder Funk weitergegeben werden.

>> SSID (Service-Set-Identifier) – ist eine Folge von Zeichen (Netzwerkname), die ein WLAN eindeutig benennt. Eine SSID ist der Name eines WLAN-Netzwerkes, das auf der IEEE-Norm 802.11 basiert. Die Liste der SSIDs (Namen) wird z. B. im Smartphone als Liste der WLANs in der Nähe angezeigt.

WLAN-Konfiguration

► Netztrennung

Die Problemstellung der Planung und Erstellung einer sicheren Netzarchitektur beinhaltet auch Überlegungen des logischen Aufbaus. Verschiedene Benutzer- und Gerätegruppen müssen getrennt und ihre Kommunikation durch Firewall-Techniken kontrolliert werden. Für Gäste sollte grundsätzlich ein separates Netz mit eigenem *Service-Set-Identifier* (*SSID*) eingerichtet werden, das von allen anderen Netzen getrennt ist und von dem aus kein Zugriff auf betriebskritische IT-Strukturen (z. B. Management- und Buchhaltungssysteme des Hotels) zugelassen wird. Auch für weitere Bereiche eines Hotels, die voneinander getrennt werden sollen, sind separate *SSID* mit eigenen Netzwerkrichtlinien einzurichten. Da eine Funkübertragung aus sicherheitstechnischer Sicht allerdings immer kritischer zu sehen ist als eine kabelbasierte Übertragung, sollte immer die Frage nach der Notwendigkeit für einen drahtlosen Netzzugang gestellt werden.

► Verschlüsselung

Zur Absicherung des Datenverkehrs über WLAN wurden mehrere Verschlüsselungsverfahren entwickelt. Das Mindestmaß stellt *WPA* dar. Für einen effektiven Schutz von WLAN sollte aber die weiterentwickelte Version *WPA2* in Verbindung mit einem *Pre-Shared Key (PSK)* zum Einsatz kommen. Seit Juni 2018 ist als Ergänzung zu *WPA2* der neue Standard *WPA3* verfügbar.

12 Dateiübertragung über WLAN

► Authentifizierung / Zugang zum WLAN

Grundsätzlich ist es natürlich möglich, das Gäste-WLAN unverschlüsselt bereitzustellen und die Absicherung der Kommunikation den Gästen zu überlassen. Allerdings ergibt sich aus der rechtlichen Problematik der „Störerhaftung“ eine Notwendigkeit zur Implementierung eines Zugangsmechanismus über den notfalls ein/eine bestimmter/bestimmte Nutzer/in identifiziert werden kann (Vbl. Cyberdyne; Zugriff 08/2019).

Ein Zugang kann beispielsweise über ein *Captive Portal* mit Anbindung einer zentralen Benutzerverwaltung (*RADIUS*-Server) realisiert werden. Die Zugangsdaten können den Gästen hierbei in Form eines Vouchers (z. B. auch in Form eines QR-Codes), der Zusendung via SMS oder E-Mail bzw. einem vereinbarten Nutzernamen, z. B. E-Mail Adresse bereitgestellt werden). Der RADIUS-Server übernimmt dabei für den Service die Authentifizierung, das heißt die Überprüfung einer individuellen Benutzername / Kennwort Kombination.

>> Captive Portal ist eine Website, die zum Zwecke der Authentifizierung, Zahlung, Annahme eines Endbenutzerlizenzvertrags oder der Darstellung von Richtlinien usw. angezeigt wird, bevor dem/der Benutzer/in des (W)LANs, ein breiterer Zugriff auf Netzwerkressourcen (z. B. das Internet) gewährt wird. RADIUS-Protokoll (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Authentifizierung, Autorisierung und zum Accounting von Benutzern/innen in ein Computernetzwerk dient.

Nutzungsbedingungen

Um den rechtlichen Anforderungen zu genügen, müssen die Gäste verständlich und transparent über die Nutzung des Gäste-WLAN informiert werden. Dies kann beispielsweise durch Nutzungsbedingungen geschehen, die zumindest die folgenden Bereiche thematisieren:

- Leistungen des Hotels (z. B. Art, Umfang, Verfügbarkeit der Leistung, hier sollte beispielsweise auch der Anspruch der Gäste auf ein funktionsfähiges Internet verneint sowie auf die Kosten eingegangen werden)
- Zugang, Zugangsdaten und Nutzung
- Pflichten als Nutzer/in und Verbote (mit expliziten Hinweis darauf, dass keine Rechtsverletzungen begangen werden dürfen)
- Rechte des Hotels, Haftungsfreistellung und Haftungsbeschränkung
- Datenschutz (hier muss auch darauf hingewiesen werden, dass durch die Verbindung Kommunikationsdaten bzw. Protokolldaten temporär gespeichert werden)
- Schlussbestimmungen (Gerichtsstand, Salvatorische Klausel)

Da es sich bei Nutzungsbedingungen um allgemeine Geschäftsbedingungen handelt, die den Vorschriften der §§ 305 ff. BGB (Bürgerliches Gesetzbuch) unterliegen, sollte die inhaltliche Gestaltung auf jeden Fall im Rahmen einer Rechtsberatung erfolgen und muss natürlich auf die jeweiligen Gegebenheiten zugeschnitten sein.

>> Für einen Überblick über die Gefährdungslage eines WLAN sowie grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs aufgebaut und betrieben werden, kann beispielsweise Baustein NET 2.1 des BSI Grundschutzkompendiums konsultiert werden (Vgl. BSI; Zugriff 08/2019).

>> Mehr Information zum Thema „Datenschutz und IT-Sicherheit in der Hotellerie“ sowie weitere Anwendungsbeispiele wie Hotel Management, Zugang zum Zimmer oder Sprachsteuerung, sind im „Leitfaden SMART Hotel“ auf den Seiten 118-135 zu finden.

ABBILDUNGSNACHWEISE

Umschlag vorne: pixabay.com/de (Stand 09/2019)

1, 4, 6, 8, 9, 11, 12: pixabay.com/de (Stand 09/2019)

2, 3, 5, 7: Eigene Darstellung

10: Eigene Darstellung, in Anlehnung an PwC: Cyber and data security in the hotel industry, URL: https://www.pwc.com/m1/en/publications/documents/cyber-and-data-security-in-the-hotel-industry.pdf (09/2019)
Umschlag hinten: Innitiative Mittelstand 4.0 (Stand 10/2019)

LITERATURVERZEICHNIS

Bundesamts für Sicherheit in der Informationstechnik (BSI): Cyberglossar, URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html (Stand 08/2019)

Bundesamts für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz,
URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html (Stand 08/2019)

Bundesanzeiger Verlag GmbH: Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU), URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl119s1626.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s1626.pdf%27%5D__1593607015760 (Stand 07/2020)

Bundesministerium der Finanzen: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), URL: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html (Stand 07/2020)

Bundesministerium der Justiz und für Verbraucherschutz: Bundesdatenschutzgesetz (BDSG),
URL: https://www.gesetze-im-internet.de/bdsg_2018/ (Stand 07/2020)

Bundesministerium der Justiz und für Verbraucherschutz: Bürgerliches Gesetzbuch (BGB),
URL: https://www.gesetze-im-internet.de/bgb/ (Stand 07/2020)

Bundesministerium der Justiz und für Verbraucherschutz: Handelsgesetzbuch (HGB),
URL: https://www.gesetze-im-internet.de/hgb/ (Stand 07/2020)

Bundesministerium der Justiz und für Verbraucherschutz: Telemediengesetz (TMG),
URL: https://www.gesetze-im-internet.de/tmg/ (Stand 07/2020)

Cyberdyne: Abschaffung der WLAN-Störerhaftung. Was das für Betreiber freier WLAN Hotspots bedeutet,
URL: https://www.youtube.com/watch?v=thUI5PrZ0vo (Stand 08/2019)

EUR-Lex: Datenschutzgrundverordnung (DSGVO),
URL: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (Stand 07/2020)

Hotel News Now: Timeline: The growing number of hotel data breaches,
URL: https://www.hotelnewsnow.com/Articles/50937/Timeline-Thegrowing-number-of-hoteldata-breaches (Stand 08/2019)

IT-Administrator: pre-shared key, URL: https://www.it-administrator.de/lexikon/pre-shared_key.html (Stand 08/2019)

KINAST Rechtsanwaltsgesellschaft mbH: www.datenschutzticker.de (Stand 08/2019)

Kompass Informationssicherheit und Datenschutz, URL: https://www.kompass-sicherheitsstandards.de/ (Stand 08/2019)

Security Standards Council, URL: https://www.pcisecuritystandards.org/ (Stand 08/2019)

MITTELSTAND 4.0 - KOMPETENZZENTRUM ROSTOCK

Mittelstand 4.0-Kompetenzzentrum Rostock ist Teil der durch das Bundesministerium für Wirtschaft und Energie geförderten Initiative Mittelstand Digital und bietet Unterstützung bei allen Fragen rund um die Digitalisierung unternehmerischer Prozesse. Expertinnen und Experten begleiten kleine und mittelständische Unternehmen aus Mecklenburg-Vorpommern auf dem Weg von einem analogen in einen digitalen Arbeitsalltag und zeigen Chancen und Lösungsmöglichkeiten des digitalen Wandels auf.

Kontakt

Mittelstand 4.0 – Kompetenzzentrum Rostock
Deutsche Med Platz 1
18057 Rostock

Tel.: 0381 494 7378
E-Mail: info@kompetenzzentrum-rostock.digital

Web: www.kompetenzzentrum-rostock.digital

IMPRESSUM

Verlegerin:
Hochschule Wismar
University of Applied Sciences: Technology, Business and Design
Philipp-Müller-Straße 14
23966 Wismar

Telefon: 03841 753 0
Telefax: 03841 753 7383
Internet: www.hs-wismar.de

Rechtsform:
Die Hochschule Wismar ist eine Körperschaft des Öffentlichen Rechts.

Vertretung:
Vertretungsberechtigter gemäß § 79 LHochSchG:
Prof. Dr. jur. Bodo Wiegand-Hoffmeister (Rektor der Hochschule Wismar)

Zuständige Aufsichtsbehörde:
Ministerium für Bildung, Wissenschaft und Kultur des Landes Mecklenburg-Vorpommern
Werderstraße 124
19055 Schwerin

Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz:
DE 183844642

Soweit keine redaktionelle Kennzeichnung für den Inhalt Verantwortlicher gem. § 55 II RStV:
Prof. Martin Wollensak
Philipp-Müller-Straße 14
23966 Wismar

Projektleitung:
Prof. Martin Wollensak
Prof. Dr. Antje Raab-Düsterhöft

Redaktion:
B. Eng. Kirsten Bayer Gersmann
B.A. Annika Borchert
B.A. Frauke Nessler
Ing. arch. Lucia Oberfrancová

Gestaltung und Produktion:
Ing. arch. Lucia Oberfrancová
B.A. Annika Borchert

Beratung:
Prof. Dr. Matthias Wißotzki
Herr Dirk Klein (Hotel & Ferienanlage Haffhus GmbH)

Druck:

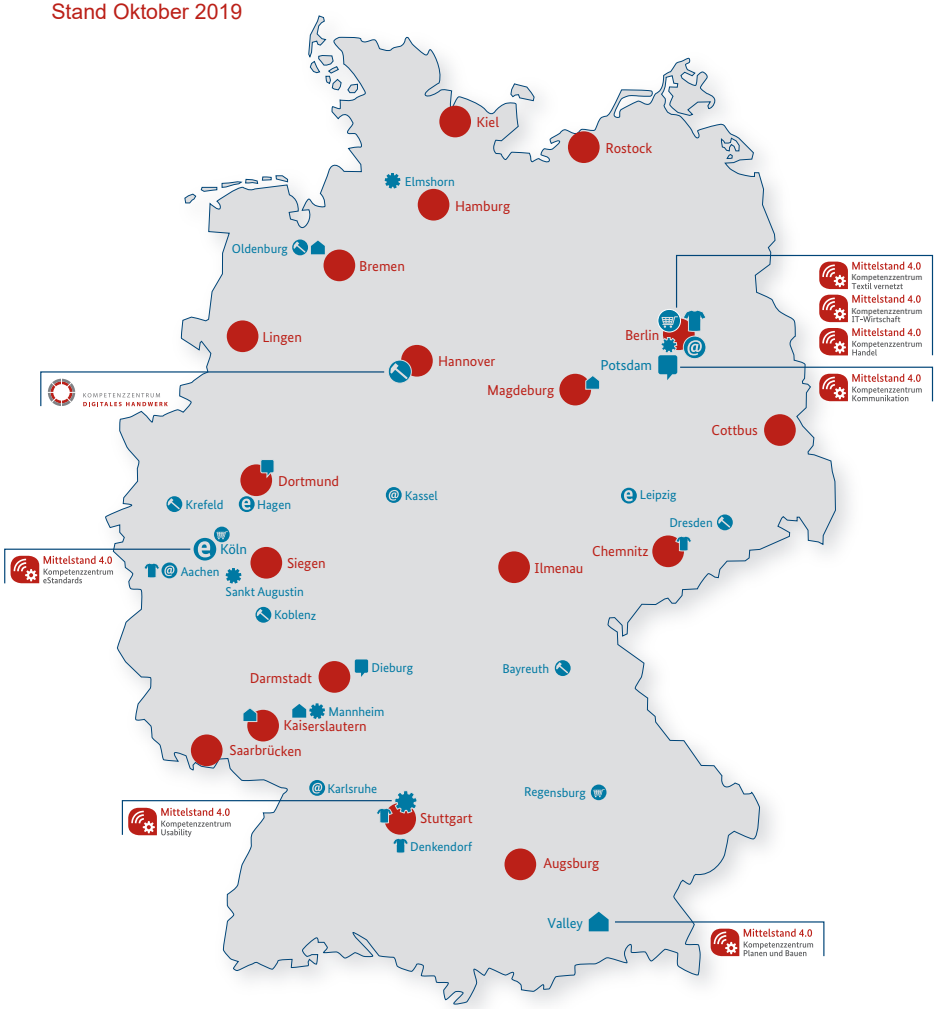
1. Auflage, Stand Juni 2020

Im Auftrag der Hochschule Stralsund im Rahmen des Projektes Mittelstand 4.0-Kompetenzzentrum Rostock

Die in diesem Themenheft enthaltenen Informationen sind für Kleine und Mittlere Unternehmen im Hotel- und Gastgewerbe bestimmt; sie erheben weder Anspruch auf Vollständigkeit noch auf Richtigkeit und entsprechen dem allgemeinen Wissensstand Anfang 2020. Die Ausarbeitung geht in einigen Bereichen neue Wege, die noch nicht in allen Bereichen wissenschaftlich belegbar sind.

ÜBERSICHTSKARTE MITTELSTAND 4.0 KOMPTENZZENTREN UND THEMENZENTREN

Stand Oktober 2019



Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best Practice Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

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