Mittelstand 4.0
Kompetenzzentrum
Planen und Bauen

Praxis

Mobile Endgeräte im Handwerksbetrieb

Nutzung von Smartphones und Tablets im Arbeitsalltag
sicher und DS-GVO-konform

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Smartphone, Tablet & Co. im Betrieb einsetzen – aber sicher!

Mobile Endgeräte wie Smartphones, Tablet-PC, aber auch Wearables wie Smartwatches haben längst Einzug gehalten in die alltägliche Arbeit im Handwerk. Vielfach setzen die Mitarbeiter ihre eigenen, privat angeschafften und unterhaltenen Smartphones auch für betriebliche Zwecke ein. Das ist mit Vorteilen, aber auch ganz praktischen sowie rechtlichen Problemen behaftet.

Nachfolgend zeigen wir Ihnen einige grundlegende Aspekte des Smartphone- und Tablet-Einsatzes im Handwerksbetrieb auf, damit Ihre Kommunikation praktisch und rechtlich einwandfrei läuft.

Mobile Endgeräte sind immer dabei – aber mit Sicherheit!

Der Vorteil von Smartphone und Tablet ist, dass man sie überall hin mitnehmen kann. Ihre Funktionen sind stets verfügbar. Der Informationsfluss gerät nie ins Stocken und vorbei sind die Zeiten, in denen eine Nachricht an den Chef auf dem Weg von der Baustelle in die Firma verloren ging.

Mit diesen Vorteilen gehen andererseits besondere Risiken einher, die vor dem Einsatz mobiler Endgeräte nahezu oder völlig unbekannt waren. So kann ein Moment der Unaufmerksamkeit genügen und das Gerät wird von einem Fremden benutzt oder sogar gestohlen.

Als Diebesgut sind die in der Anschaffung recht hochpreisigen Geräte sehr beliebt. So berichtete das Presseportal bereits 2016, dass allein in Deutschland jeden Tag fast 600 Handys gestohlen werden. Ist das Gerät erstmal weg, kann unter anderem:

- Einblick in Daten wie dem Adressbuch, in SMS sowie ggf. auch E-Mails oder einem via App erreichbaren elektronischem Ressourcen-Management (ERM-System) erhalten werden
- Spionage-Apps installiert und so das Gerät und seine Nutzung ausgespäht und überwacht werden
- kostenpflichtige Dienste zu Lasten des Anschlussinhabers gentutz werden
- auf dem Gerät gespeicherte Zugangsdaten zum eigenen Vorteil genutzt werden, um z.B. Waren auf Kosten des Account-Inhabers zu ordern
- gefälschte Nachrichten an Kunden und Kollegen versendet werden

Die hier aufgeführten Risiken sind nicht lediglich theoretischer Natur, auch wenn in einer hohen Zahl der Fälle der Dieb einen Gewinn durch den Weiterverkauf des Geräts oder einzelner Komponenten erzielen möchte.

Impressum

Herausgeber: Mittelstand 4.0-Kompetenzzentrum Planen und Bauen / eBusiness-Kompetenzzentrum gUG (haftungsbeschränkt), Fraunhofer-Institut für Bauphysik IBP (Gesamtleitung), Fraunhofer Straße 10, 83626 Valley
Redaktion: Michael Weller (Autor), m.weller@ebusiness-kompetenzzentrum.de; Telefon: 0631-205 601 801
Gestaltung und Produktion: buildingSMART Deutschland, Wiener Platz 6, 01069 Dresden
Bildnachweis: Alle Bilder: www.pixbay.com, lizenziert unter CCO Public Domain Dedication, Lizenzbedingungen abrufbar unter: https://creativcommons.org/publicdomain/zero/1.0/deed.de
Online: verfügbar als PDF-Download unter: www.kompetenzzentrum-planen-und-bauen.digital - Stand: August 2018

Die 10 Gebote der Smartphone-Sicherheit

Um diesen Risiken zu begegnen raten unter anderem Datenschutzaufsichtsbehörden dazu:

- Fingerabdruck, PIN und Passwort zu verwenden, um einerseits die SIM-Karte im Smart-phone oder Tablet gegen unbefugte Nutzung des Telekommunikationsnetzes abzusichern und andererseits die Displaysperre aufzuheben
- sie Funktion der automatischen Zugriffssperre zu nutzen und in den Geräteeinstellungen die Zeit bis zu deren Aktivierung nicht über das erforderliche Maß hinaus auszudehnen
- Standortdienste, die Informationen über den Ort erhalten, an dem sich das Smartphone befindet, manuell und sinnvoll zu konfigurieren, d.h. nur dann zu verwenden, wenn dies erforderlich und hilfreich ist
- Sicherheitstechniken nicht mehr als unbedingt erforderlich durch einen Rooting-Versuch oder die Aktivierung von Entwickleroptionen aus-zuhebeln
- regelmäßig Software-Updates durchzuführen
- Vorkehrungen für sinnvolle Sicherungskopien (Backups) zu treffen
- Apps nur nach vorheriger Prüfung und erst dann zu installieren, wenn man ihre Funktion verstanden hat
- bei einem Verlust des Geräts, unverzüglich die SIM-Karte beim Mobilfunkanbieter sperren zu lassen und einen Diebstahl bei der örtlichen Polizeidienststelle anzuzeigen
- bei einem Verlust die Ortungsfunktion des Gerätes zum Wiederauffinden zu nutzen
- bei einem Verkauf des Geräts, Speichermedien wie z.B. SD-Karten zu entfernen – soweit dies möglich ist – und das Gerät von persönlichen Informationen befreien sowie auf die Werkseinstellungen zurückzusetzen

Die Umsetzung der 10 Gebote im Handwerksbetrieb

Wie diese zehn Gebote im Handwerksbetrieb umgesetzt werden können, hängt von der Nutzungskultur mobiler Endgeräte im jeweiligen Betrieb ab. Man kann im Grundsatz drei verschiedene Nutzungskulturen unterscheiden:

Dienstgerät zur ausschließlich dienstlichen Nutzung

Diese Variante, in der ein dienstlich durch den Betrieb an die Mitarbeiter ausgegebenes Endgerät nur zu dienstlichen Zwecken benutzt werden darf, ist praktisch und rechtlich die am einfachsten zu fassende Konstellation. Denn in einer Überlassungsvereinbarung können die Unternehmer die Nutzung dieses Dienstgeräts recht detailliert regeln. Von dieser Befugnis sollten sie auch unbedingt Gebrauch machen. So können und sollten insbesondere Festlegungen getroffen werden in Bezug auf:

- das überlassene Gerät nach Typ, Seriennummer, IMEI sowie eingelegter SIM-Karte und ggf. eingelegten Speichermedien wie einer SD-Karte o.ä.
- PIN- und Passwort-Richtlinien zur Anwendung und Generierung sicherer Sperren und Passwörter
- die Berechtigungen zum Installieren von Apps
- die Berechtigungen zur Nutzung von Kommunikationsdiensten wie Telefonie, SMS, Internet
- die (De-)Aktivierung von Ortungsfunktionen insbesondere während Pausenzeiten und nach Feierabend sowie im Urlaub
- die (De-)Aktivierung von Diensten oder des Roaming bei Auslandsaufenthalten
- die Kontrolle der Abrechnung und der Gerätenutzung
- die Vorgehensweise bei Beschädigung oder Verlust des Geräts
- die Überlassungsdauer

Ist ein Betriebsrat vorhanden, ist dieser zu involvieren. Die Geräte sind grundsätzlich zur Leistungsüberwachung geeignet, so dass hier frühzeitig über den Einsatz ein Einvernehmen erzielt werden sollte.

Die Nutzung des privaten Handys ist in einem solchen Fall regelmäßig nicht vollständig zu untersagen. Sie kann jedoch zeitlich, z.B. auf Pausenzeiten, oder räumlich, z.B. auf Bereiche außerhalb der Beeinflussbarkeit empfindlicher Messinstrumente, eingeschränkt werden, soweit eine Erreichbarkeit im Notfall gegeben ist. Das führt dann allerdings dazu, dass die Mitarbeiter – was nicht sehr beliebt ist – zwei Geräte bei sich tragen.

Privatgerät mit dienstlicher Nutzung

Diese Konstellation ist praktisch wie rechtlich die kritischste, denn das private Endgerät muss in die IT-Struktur des Unternehmens eingebunden werden und es muss sichergestellt werden, dass betriebliche Daten nicht mit privaten Daten vermischt werden. Das gelingt aber schon nicht, wenn der Mitarbeiter vom Privathandy beim Kunden anruft, dem die Rufnummer des Anrufers angezeigt wird.

Darüber hinaus kann der Betrieb nicht festlegen, wie die Eigentümer mit einer Beschädigung oder einem Verlust des Geräts umzugehen haben. Ferner kann nicht festgelegt werden, welche Bereitschaftszeiten zu gewährleisten sind, welche Anti-Viren-Software eingesetzt wird und dem Eigentümer kann auch nicht untersagt werden, aus Firmensicht kritische Apps zu installieren. Schließlich darf ein Arbeitgeber das Privatgerät nicht ohne weiteres kontrollieren oder gar an sich nehmen.

Sollen Firmenapplikationen auf dem Gerät installiert werden, muss zunächst mit den Anbietern der Apps die Frage geklärt werden, ob dies zulässig ist. Bestehen zahlenmäßig begrenzte Lizenzen kann insbesondere bei etwas höherer Mitarbeiterfluktuation das Volumen schnell ausgeschöpft und eine weitere Installation auf dem Gerät eines neuen Mitarbeiters lizenzwidrig sein. Eine lizenzwidrige Installation führt in der Regel zu hohen Schadensersatzansprüchen des Lizenzgebers gegen den Betrieb.

Kann über eine Firmenapplikation auf betriebliche Daten wie z.B. die Kundendatenbank zugegriffen werden, besteht für den Betrieb das Risiko, dass über das Mitarbeiter-Smartphone ein unerwünschter und datenschutzrechtlich unzulässiger Datentransfer erfolgt. Dies ist zum Beispiel der Fall, wenn der Mitarbeiter den Dienst WhatsApp nutzt und gleichzeitig Kundenrufnummern im Adressbuch seines Handys speichert.

Eine betriebliche Nutzung von WhatsApp sehen die Datenschutzaufsichtsbehörden solange als unzulässig an, bis der Betrieb zu allen im Speicher des Geräts gespeicherten Kunden nachweisen kann, dass diese aktiv – d.h. auf Nachfrage des Betriebes – der Nutzung dieses Dienstes zugestimmt haben. Eine Zustimmung des Kunden liegt nach Ansicht von Datenschutzexperten u.U. auch dann noch nicht vor, wenn dieser den Betrieb zur Kontaktaufnahme über diesen Dienst auffordert.

Das bedeutet, der Betrieb muss die aktive Zustimmung vom Kunden erbitten und wenn diese erteilt wird, entsprechend dokumentieren und das auch von Kunden, die den Dienst selbst gar nicht nutzen.

Technisch möglich sind heute schon so genannte Container-Lösungen. Diese bieten die Möglichkeit, betriebliche Daten von den privaten getrennt zu verarbeiten. Die Verarbeitung der betrieblichen Daten geschieht dann in einem virtuellen Container auf dem jeweiligen privaten Endgerät. Dadurch ist aber der beschriebene manuelle Transfer der Rufnummer eines Kunden in das private Telefonbuch des Eigentümers nicht ausgeschlossen. Gerät eine solche Information z.B. an WhatsApp, kann ein meldepflichtiges Datenleck vorliegen, das neben Geldbußen einen massiven Vertrauensverlust bei den Kunden zur Folge hat.

Ebenfalls möglich ist die Benutzung einer zweiten dienstlichen Rufnummer neben der privaten Rufnummer auf einem Gerät. Dieses muss dann aber Dual-SIM-fähig sein. Den Mitarbeitern ist jedoch betrieblich keine Vorgabe zu machen, welche Geräte sie sich privat beschaffen, so dass es hier auf die Mitwirkung der Mitarbeiter ankommt.

Allein diese Beispiele machen bereits deutlich, dass der administrative Mehraufwand die Ersparnis der Anschaffung von Geräten durch den Betrieb leicht aufzehren kann. Vereinbarungen zur Bereitstellung privater Endgeräte im Unternehmen – auch unter dem Begriff „Bring your own Device“ bzw. der Abkürzung „BYOD“ bekannt – sind in aller Regel sehr komplex und können ohne fundierte juristische Expertise kaum rechtssicher ausgestaltet werden. Das aber macht die Vereinbarungen teuer.

Dienstgerät zur dienstlichen und zur prviaten Nutzun

Als denkbarer Mittelweg kann sich anbieten, an die Mitarbeiter betriebseigene Geräte auszugeben, die privat genutzt werden dürfen. In einem solchen Fall ist das Unternehmen Eigentümer des Geräts und kann daher über die Anschaffung frei entscheiden. Ferner bestehen aufgrund der Anschaffungsentscheidung keine über das allgemeine Maß hinausgehenden Schwierigkeiten, die Geräte in die IT-Infrastruktur des Betriebes einzubinden und gegen Angriffe durch Dritte abzusichern.

Allerdings muss das Unternehmen bedenken, dass für Arbeitgeber anders als im Falle der rein betrieblichen Nutzung keine umfassenden Kontrollbefugnisse mehr bestehen. Diese sind im Wesentlichen auf folgende Konstellationen beschränkt:

- es besteht der konkrete Verdacht, dass das Endgerät zur Begehung einer oder mehrerer Straftaten verwendet wurde
- es besteht der konkrete Verdacht, dass das Endgerät erheblich über das vereinbarte Maß hinaus exzessiv genutzt wurde

Diese Beschränkung geht für die Arbeitgeber mit dem Vorteil einher, dass sie von ihrer Kontrollverpflichtung auch in Bezug auf die Untersagung der privaten Nutzung frei werden. Das bedeutet konkret: ist die private Nutzung untersagt, muss dieses Verbot auch durch Kontrollen und bei festgestellten Verstößen durch das Ergreifen arbeitsrechtlicher Maßnahmen, z.B. dem Aussprechen einer Abmahnung durchgesetzt werden – dies entfällt hier.

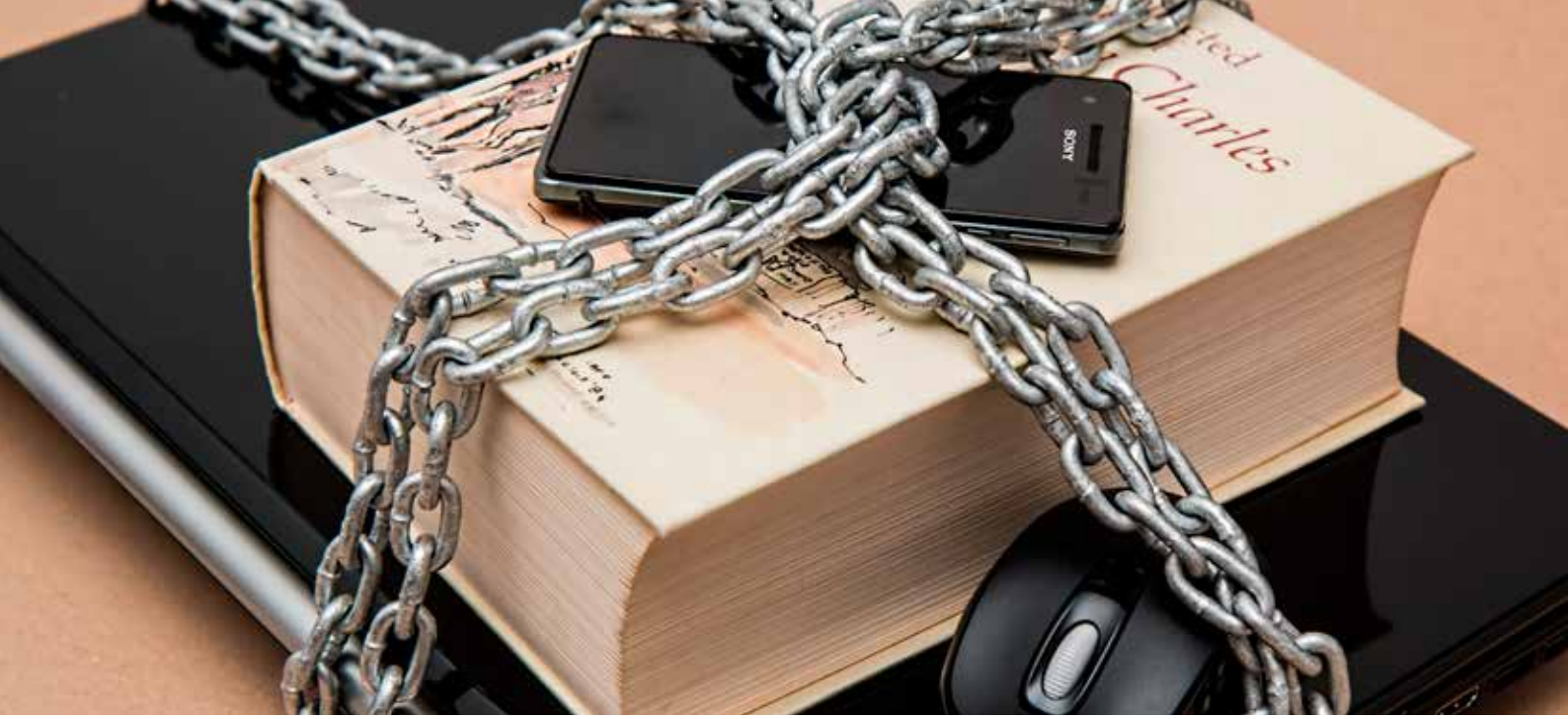
Trotzdem sind den Unternehmern die Hände nicht gebunden. Sie können das Beschäftigungsverhältnis beenden, wenn:

- die betreffenden Mitarbeiter arbeitsvertragliche Pflichten durch exzessives privates Nutzen des dienstlich überlassenen Geräts verletzen oder
- die betreffenden Mitarbeiter – selbst außerhalb der Arbeitszeit – eine Straftat begehen, die zur Aufgabe des Unternehmens in Widerspruch steht

Die eingangs vorgestellte Vereinbarung über die Nutzung des dienstlichen Gerätes muss allerdings im Hinblick auf die private Nutzung ergänzt werden. Insbesondere sollte zusätzlich folgendes einer Regelung zugeführt werden:

- in welchem Umfang ist eine private Nutzung des Geräts erlaubt
- wie ist die Verteilung der Kosten oder übernimmt der Betrieb diese vollständig
- bei welchen Gelegenheiten und in welchem Umfang wird die Gerätenutzung und das Gerät selbst kontrolliert
- in welchen Fällen muss das Gerät zurückgegeben werden oder dem Betrieb wieder zur Verfügung gestellt werden
- wie ist mit privaten Nachrichten zu verfahren, die auf dem Gerät eingehen, z.B. Kennzeichnungs- oder Weiterleitungsregeln.

Auch hier ist das Betriebsverfassungsrecht zu beachten und ein etwa bestehender Betriebsrat möglichst frühzeitig einzubeziehen. Dadurch können vor allem auch Akzeptanz- und Auslegungshürden erheblich abgesenkt oder ganz vermieden werden.



Vor- und Nachteile der Nutzungskulturen auf einen Blick

	Dienstgerät zur ausschließlich dienstlichen Nutzung	Privatgerät mit dienstlicher Nutzung	Dienstgerät zur dienstlichen und privaten Nutzung
DS-GVO-Konformität	Kein Vermischen betrieblicher und privater Daten möglich	Schwierige Einbindung privater Hardware in betriebliche IT-Sicherheit	TechnischeMaßnahmen arbeitgeberseitig erforderlich und möglich
Schutz von Betriebs- und Firmengeheimnissen	Daten bleiben auf dem Gerät o. in zugriffsrechtbezogenene Räumen	Schwierige Einbindung privater Hardware in betriebliche IT-Sicherheit	Technische Maßnahmen arbeitgeberseitig erforderlich und möglich
Gerätehoheit	Besitz:Mitarbeiter Eigentum: Betrieb	Besitz: Mitarbeiter Eigentum: Mitarbeiter	Besitz: Mitarbeiter Eigentum: Betrieb
Sonderanforderungen	Nutzungsvereinbarung mit Direktionsrecht - leicht in Abstimmung zubringen - Akzeptanzhürde bei den Mitarbeitern zu überwinden	Nutzungsvereinbarung komplex, technisch aufwändige Einbindung privater Geräte - in der Regel hohe Mitarbeiter-Akzeptanz	Nutzungsvereinbarung unwesentlich komplexer als im Fall rein dienstlicher Nutzung - in der Regel ordetnliche Akzeptanz im Betrieb
Arbeitgeber (+)	(Fast) vollständige Kontrolle über Gerät und Nutzung und Sicherheit	Keine Anschaffung von und Stellung von Infrastruktur erforderlich	Bestimmung der grundlegenden Geräte- und Sicherheitskonfiguration
Arbeitgeber (-)	Beschaffungsaufwand und Akzeptanzproblem im Betrieb	(Fast) keine Kontrolle über Gerät und Nutzung sowie IT-Sicherheit	Beschaffungsaufwand und Einschränkung der Kontrollrechte
Mitarbeiter (+)	Keine Notwendigkeit, private Infrastruktur zu stellen	Keine Ungewöhnung auf dienstliches Gerät und System erforderlich	Keine Notwendigkeit, zweites Gerät mitzuführen oder bereitzuhalten
Mitarbeiter (-)	Für private Nutzung Privatgerät zusätzlich mitzuführen	Notwendigkeit, private Infrastruktur zur Verfügung zu stellen	Begrenzte Verfügbarkeit im Rahmen der Nutzungsvereinbarung

Dokumentation des IT-Einsatz

Gleich, wie die Entscheidung für eine und gegen die anderen Unternehmenskulturen in Bezug auf die Benutzung mobiler Endgeräte im Unternehmen auch ausfällt, eins muss das Unternehmen stets leisten: Die Verwendung von mobilen Endgeräten und der auf diesen installierten Applikationen muss im Verzeichnis der Verarbeitungstätigkeiten beschrieben werden. Dieses Verzeichnis ist von allen Handwerksbetrieben zu führen, die mindestens einen Angestellten haben. Das bedeutet, dass auch die Ein-Mann-GmbH ein solches Verzeichnis führen muss, denn für den Juristen ist die GmbH eine von ihrem Geschäftsführer und einzigen Angestellten abweichende, also eine andere Person.

Welche Informationen in dieses intern zu führende Verzeichnis aufzunehmen sind, ergibt sich aus der Regelung in Art. 30 der europäischen Datenschutz-Grundverordnung (DS-GVO = VO (EU) 2016/679).

Werden darüber hinaus steuerrelevante Unterlagen mittels der mobilen Endgeräte be- oder verarbeitet, müssen diese Geräte auch in der Verfahrensdokumentation nach den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) berücksichtigt werden. Bei den GoBD handelt es sich um ein Schreiben des Bundesministeriums der Finanzen vom 14.11.2014 an die obersten Finanzbehörden der Länder. In diesem ist unter Ziffer 10.1 beschrieben, welche Anforderungen an die Dokumentation des Umgangs mit steuerrelevanten Unterlagen im Betrieb gestellt werden.

Quellen:

Presseportal zur Zahl der Smartphone-Diebstähle in Deutschland:
https://www.presseportal.de/pm/55928/3348558

Bayerisches Landesamt für Datenschutzaufsicht zur Sicherheit exemplarisch für Android-Geräte:
https://www.lda.bayern.de/media/flyer_android.pdf

und für Apple-Geräte:
https://www.lda.bayern.de/media/flyer_ios.pdf

Die Landesbeauftragte für den Datenschutz in Niedersachsen zur Nutzung von WhatsApp im Betrieb
https://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/nutzung_von_whatsapp_im_unternehmen/merkblatt-fuer-die-nutzung-von-whatsapp-in-unternehmen-166297.html

Bundesministerium der Finanzen, GoBD v. 14.11.14:
https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.html

---

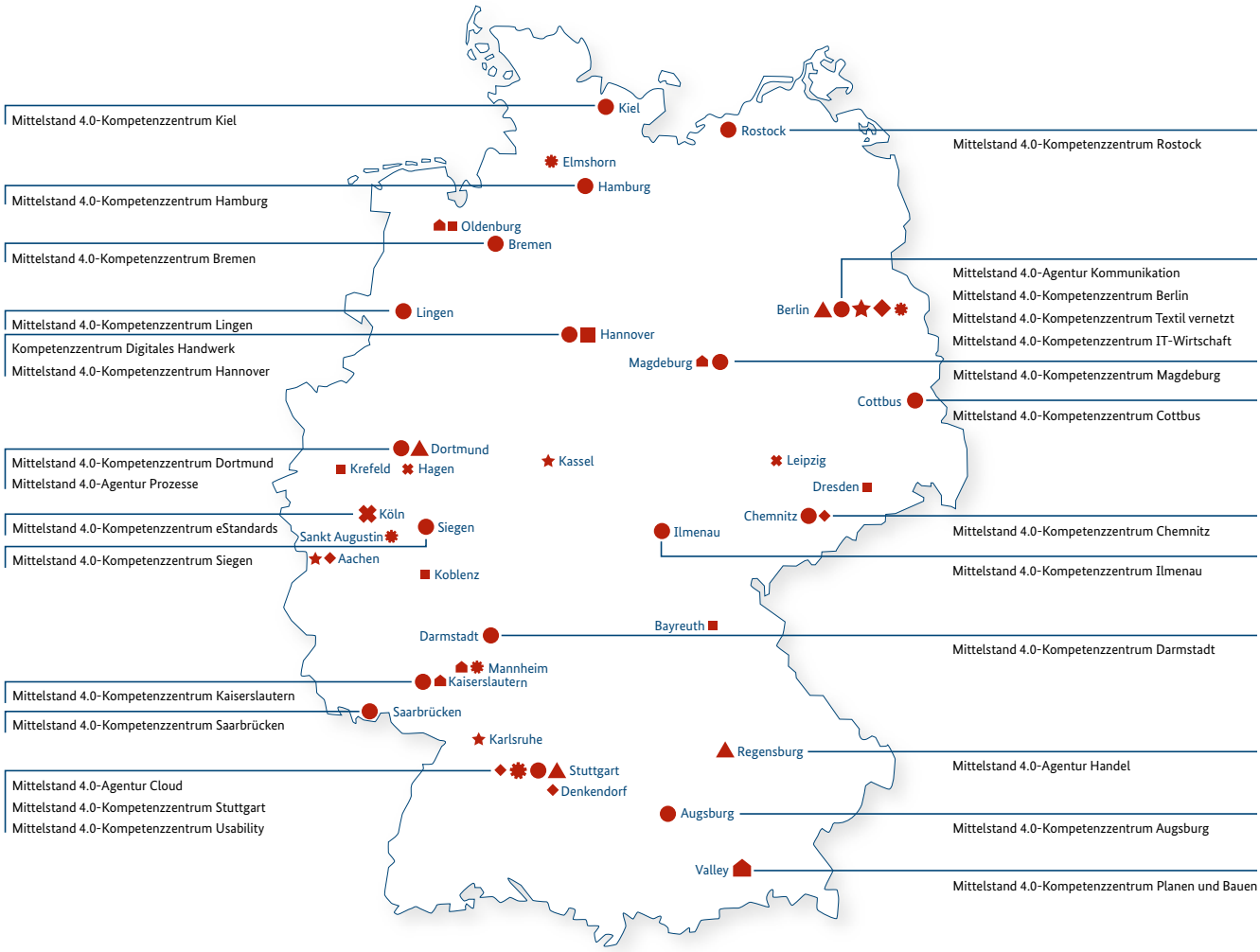
Kontakt:

Haben Sie Fragen zum Thema „Mobile Endgeräte im Handwerksbetrieb“ oder zum Erstellen und Führen von Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO sowie der Verfahrensdokumentation nach GoBD, so wenden Sie sich an unsere Experten.

Ihr Ansprechpartner für alle Aspekte des rechts-konformen IT-Einsatzes ist:

Ass.jur. Michael Weller
Rechtsanwalt und Senior Berater IT-Compliance
eBZ - eBusiness-Kompetenzzentrum gUG (haftungsbeschränkt)
Europaallee 10
67657 Kaiserslautern
Telefon: 0631 - 20 56 01 801
E-Mail: m.weller@ebusiness-kompetenzzentrum.de

Mittelstand 4.0
Kompetenzzentrum Planen und Bauen



- Kompetenzzentren der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Agenturen der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Kompetenzzentrum Digitales Handwerk
- Regionale Schaufenster Digitales Handwerk
- Kompetenzzentrum Usability
- Regionale Anlaufstellen Usability
- Kompetenzzentrum IT-Wirtschaft
- Regionale Stützpunkte IT-Wirtschaft
- Kompetenzzentrum Textil vernetzt
- Regionale Schaufenster Textil vernetzt
- Kompetenzzentrum eStandards
- Offene Werkstätten eStandards
- Kompetenzzentrum Planen und Bauen
- Regionale Anlaufstellen Planen und Bauen

Über Mittelstand Digital

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalsierung. 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 kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

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

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages