.

14. Ergänzung Sonderrundschreiben - Corona Virus

INHALTSVERZEICHNIS

1. Aktuelle Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2

2. Auswirkungen auf den Jahresabschluss 2019

3. Ausnahmeregelung zu Arbeitsunfähigkeitsbescheinigungen per Telefon

4. IT-Sicherheit im Homeoffice

5. Übersicht über Sonderregeln für die Vergabe von Bauleistungen

6. Online-Antragstellung für Corona-Entschädigung nach § 56 Abs. 1 a Infektionsschutzgesetz

1. Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2

Zusammenfassung der Änderungen, die das Handwerk betreffen:

- Erweiterung der Kinderbetreuung, nicht ausgeschöpfte Betreuungskapazitäten dürfen belegt werden, auch wenn kein Anspruch auf Notbetreuung besteht.
- Zusammenkünfte zur beruflichen Aus- und Weiterbildung sind jetzt von den Kontaktbeschränkungen des § 3 CoronaVO ausgenommen nach § 3 Absatz 3 Nr. 1 CoronaVO und werden von den Untersagungen des § 4 ausgenommen nach § 4 Abs. 2 Nr. 10 CoronaVO. Nähere Angaben dazu finden Sie unter dem Link: www.baden-wuerttemberg.de/de/service/aktuelle-infos-zu-corona/aktuelle-corona-verordnung-des-landes-baden-wuerttemberg/ und in der Verordnung zur Öffnung von Bildungseinrichtungen Link: www.baden-wuerttemberg.de/de/service/aktuelle-infos-zu-corona/verordnung-ueber-die-wiederaufnahme-des-schulbetriebs/
- Außerdem wird die Einhaltung der Abstandsregelungen nicht mehr an den Besuch von Einrichtungen im öffentlichen Raum gekoppelt, sondern generell auf den Betrieb von Einrichtungen ausgeweitet § 3 Abs. 3 Nr. 5 CoronaVO.
- Der Betrieb von Cafes und Eisdielen wurde aus der Liste der geschlossenen Einrichtungen § 4 Abs. 1 Nr. 8 CoronaVO entfernt.
- Wichtig, die bestehenden Kontaktbeschränkungen werden bis zum 05.06.2020 weiter aufrecht erhalten.

www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/200516_CoronaVO_Konsolidierte_Fassung_ab_200518.pdf

2. Auswirkungen auf den Jahresabschluss 2019

Das IDW wertet die Corona-Epidemie als wertbegründendes Ereignis. Ein solches Ereignis müsste im Zahlenwerk des Jahresabschlusses 2019 nicht berücksichtigt werden.

Viele Unternehmen sind aktuell dabei, ihren Jahresabschluss 2019 aufzustellen, die größeren Unternehmen müssen in diesem Zusammenhang auch einen Lagebericht verfassen. Aufgrund von Fragen aus Mitgliedsbetrieben weisen wir darauf hin, dass die aktuelle Krisensituation aufgrund des Coronavirus nach Ansicht des IDW bei den im Rahmen des Jahresabschlusses vorzunehmenden Bewertungen nicht berücksichtigt werden muss.
Handelsrechtlich entscheidend für die Berücksichtigung der Folgen der Corona-Epidemie im Jahresabschluss 2019 ist, ob es sich bei der Coronoa-Epidemie um ein "wertbegründendes" oder ein "wertaufhellendes Ereignis" handelt. Das für solche Fragen zuständige Institut der Wirtschaftsprüfer (IDW) klassifiziert in seiner Verlautbarung vom 4. März 2020 die Corona-Krise als "wertbegründendes Ereignis":
Wertbegründende Ereignisse liegen vor, wenn die Ursache eines bilanziellen Sachverhalts erst nach dem Abschlussstichtag aufgetreten ist. Das ist beim Coronavirus der Fall. Es tauchte erst nach dem 31.12.2019 in Europa auf, so dass die Corona-Krise handelsrechtlich erst im Jahresabschluss 2020 bei der Bewertung berücksichtigt werden muss.
Anders verhält es sich bei "wertaufhellenden Ereignissen": Bei wertaufhellenden Ereignissen wurde zwar die Ursache für das Ereignis bereits vor dem Bilanzstichtag gelegt, das Ereignis ist aber erst zwischen Bilanzstichtag und Aufstellung des Jahresabschlusse bekannt geworden. Solche wertaufhellenden Ereignisse wären handelsrechtlich bereits im Jahresabschluss 2019 zu berücksichtigen.
Ein solcher Fall könnte zum Beispiel vorliegen, wenn sich ein ehemaliger Kunde mit einem Gewährleistungsfall Anfang Dezember 2019 an das Bauunternehmen wendet, um die zum Jahresende ablaufende Gewährleistungsfrist noch einzuhalten. Der Bauunternehmer hat zunächst Zweifel, ob er für den Schaden verantwortlich ist. Wegen der hohen Termindichte können Kunde und Bauunternehmer den Schaden aber erst im Januar 2020 besichtigen und erst nach einem Sachverständigen-Gutachten im März die Höhe richtig einschätzen. In dem im Mai aufgestellten Jahresabschluss 2019 sind dann die Ergebnisse aus dem Sachverständigen-Gutachten zu berücksichtigen, indem in entsprechender Höhe eine Rückstellung für die Beseitigung des Schadens eingestellt wird.
Nach Ansicht des IDW seien die Auswirkungen der Corona-Epidemie also im Zahlenwerk des HGB-Jahresabschlusses 2019 nicht zu berücksichtigen. Lediglich beim Anhang des Jahresabschlusses 2019 müsse geprüft werden, ob es sich bei der Corona-Krise um einen anhangpflichtigen "Vorgang von besonderer Bedeutung" handelt (HGB § 285 Nr. 33 bzw. § 314 Abs. 1 Nr. 25): Ein solcher "Vorgang von besonderer Bedeutung" liegt vor, wenn seine Auswirkungen die Adressaten des Jahresabschlusses dazu veranlassen könnten, die Unternehmensentwicklung nach dem Abschlussstichtag wesentlich anders zu beurteilen.
Bei Unternehmen, die einen Lagebericht aufstellen, sollten die Corona-Epidemie 2020 und ihre Auswirkungen auf das Unternehmen im Chancen- und Risikoteil des Lageberichts 2019 auf jeden Fall Niederschlag finden. Selbst dann, wenn ein Bauunternehmer bei Aufstellung des Lageberichts noch keine Auswirkungen der Krise spürt, sollte er darstellen, warum er davon ausgeht, dass dies im Jahr 2020 auch so bleiben wird oder ob wirtschaftliche Auswirkungen im Jahresverlauf wahrscheinlich sind und welche Maßnahmen er ergreift, um diese Auswirkungen einzudämmen.
Planungsrechnungen, die im Zuge der Unternehmensbewertung erstellt wurden, sind daraufhin zu prüfen, inwieweit sie mögliche Auswirkungen der Corona-Epidemie auf das Geschäft angemessen darstellen, und müssen ggf. angepasst werden.
Die Details sollten Unternehmen, die jetzt ihren Jahresabschluss aufstellen, unbedingt mit dem Steuerberater und/oder Wrtschaftsprüfer besprechen.

3. Ausnahmeregelung zu Arbeitsunfähigkeitsbescheinigungen per Telefon

Die Ausnahmeregelung zur telefonischen Arbeitsunfähigkeitsbescheinigung wurde nochmals (nach jetzigem Stand letztmalig) bis zum 31. Mai 2020 verlängert.

Der G-BA hat am heutigen Tag beschlossen, die befristete Sonderregelung zur telefonischen Feststellung einer Arbeitsunfähigkeit durch Vertragsärzte bis einschließlich 31. Mai 2020 zu verlängern. Danach gilt weiterhin, dass die Feststellung der Arbeitsunfähigkeit bei Versicherten mit Erkrankungen der oberen Atemwege, die keine schwere Symptomatik aufweisen, für einen Zeitraum von bis zu sieben Kalendertagen auch nach telefonischer Anamnese erfolgen kann. Bei Fortdauern der Arbeitsunfähigkeit ist eine Verlängerung im Wege der telefonischen Anamnese einmalig für einen weiteren Zeitraum von bis zu sieben Kalendertagen möglich.

Laut der Pressemitteilung des Gremiums soll es sich bei dieser nun beschlossenen Verlängerung um die letztmalige Verlängerung handeln. Nach derzeitiger Einschätzung der Gefährdungslage gelte ab dem 1. Juni 2020 wieder, dass für die ärztliche Beurteilung, ob ein Versicherter arbeitsunfähig ist, eine körperliche Untersuchung notwendig ist.

Der Beschluss zur Verlängerung der Ausnahmeregelung tritt nach Nichtbeanstandung durch das Bundesministerium für Gesundheit und Veröffentlichung im Bundesanzeiger mit Wirkung vom 19. Mai 2020 in Kraft.

4. IT-Sicherheit im Homeoffice

Cyber-Kriminelle nutzen die Corona-Krise verstärkt für Angriffe. Das BSI hat deshalb Checklisten zur Sicherung der IT-Systeme zusammengestellt, wenn ein Großteil der Mitarbeiter vorübergehend ins Homeoffice wechselt.

Wir berichteten zuletzt über die Möglichkeiten von Homeoffice in Zeiten mit corona-bedingten Einschränkungen des Betriebs.

Beim Übergang ins Homeoffice muss der "Faktor Mensch" als Gefahr für die IT-Sicherheit der Unternehmens-IT neu betrachtet werden. Denn in der aktuellen Corona-Epidemie haben Cyber-Krimielle leichtes Spiel: Eine hohe Besorgnis der Bürger in Kombination mit einem hohen Informationsbedürfnis ist der ideale Nährboden, um IT-Nutzer in die Irre zu führen. Mit Hilfe von Phishing-Mails oder Smartphone-Apps können Geräte leicht mit Schad-Software infiziert werden. Folgen sind

- unseriöse Angebote zum Schutz vor den Auswirkungen der Pandemie,
- der Diebstahl von Zahlungsdaten,
- das Abgreifen persönlicher Informationen oder
- das Lahmlegen der Geräte mit anschließender Erpressung.

Gerade im Homeoffice besteht die Gefahr, dass sich Cyberkriminelle Zugang zum IT-Netzwerk des Arbeitgebers verschaffen. Das kann leichter passieren, wenn Mitarbeiter berufliche und private Tätigkeiten vermischen und die genutzten Endgeräte mit dem Unternehmen verbunden sind.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher einen Katalog von kurzfristig realisierbaren Maßnahmen erarbeitet, die gewährleisten sollen, dass in kleinen und mittelständischen Betrieben, deren Mitarbeiter erstmals im Homeoffice arbeiten, eine grundlegende IT-Sicherheit eingehalten werden kann. Mit den genannten Maßnahmen sollen die grundlegenen Ziele der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) wirksam umgesetzt werden.
Der Maßnahmenkatalog berücksichtigt allerdings nur die kurzfristige Entwicklung im Zuge der Corona-Epidemie. Im Falle einer längerfristigen Umstellung auf Homeoffice müssen weitergehende IT-Sicherheitsmaßnahmen realisiert werden (**siehe Anhang zum Notfallmanagement**).

A. Klare Regelungen für das Homeoffice vorgeben

1. Regelungen zum Umgang mit IT-Systemen und Datenträgern:
Hierzu zählen u.a. Vorgaben zu Passwörtern, Bildschirm-Sperren und mobilen Datenträgern (USB-Sticks). Unmissverständliche und verbindliche Regelungen sollten schriftlich (in Papierform) aufgestellt und an alle Mitarbeiter kommuniziert werden.

2. Organisatorische Regelungen:
- Wie muss der Arbeitsplatz gestaltet werden?
- Wie können Mitarbeiter zu Hause erreicht werden?
- Wer beantwortet Rückfragen zur IT?
- Welche Endgeräte dürfen im Homeoffice genutzt werden?
- Welche Vorgänge dürfen mit welchen IT-Anwendungen bearbeitet werden?
- Wie sollen sich die Mitarbeiter bei IT-Sicherheitsvorfällen verhalten?

3. Die Mitarbeiter sollten dazu eine Checkliste (siehe Anhang) an die Hand bekommen, mit der sie auch zu Hause für IT-Sicherheit sorgen können.

4. Erste Schritte für das sichere Homeoffice finden Unternehmer in der Checkliste im Anhang.

B. Verantwortlichkeiten für IT-Sicherheit klarstellen
Die IT-Sicherheitslage ändert sich ständig. Aktuell liegt dies auch am Coronavirus, das Cyber-Kriminelle als Aufhänger nutzen, um Phishing-Mails zu verschicken und andere Angriffe zu starten. Ein IT-Sicherheitsbeauftragter oder ein Notfallteam helfen, auf kritische Situationen schnell reagieren zu können. Sind klare Ansprechpartner benannt, können Ihre Mitarbeiter schneller Auffälligkeiten rückmelden und damit Schäden vom Unternehmen abhalten (**siehe Anhang IT-Notfallkarte**).
Private Endgeräte der Mitarbeiter können in der Regel nicht auf die IT-Sicherheitsmaßnahmen der Organisation zurückgreifen, weil sie nicht Teil der betrieblichen IT-Landschaft sind. Das Unternehmen muss darauf vertrauen, dass die Mitarbeiter selbstständig Schutzmaßnahmen wie AntiViren-Programme oder Firewalls einrichten und zeitnah Updates einspielen. Eine Checkliste erleichtert es den Mitarbeitern, an alles Notwendige zu denken (**siehe Anhang**).

C. Falls die Mitarbeiter im Home-Office unternehmenseigene Endgeräte nutzen:

1. "Härten" Sie die IT-Systeme der Mitarbeiter im Homeoffice.
Jede einzelne Funktion eines IT-Systems stellt ein potenzielles Einfallstor für Cyber-Kriminelle dar - insbesondere dann, wenn regelmäßige Updates ausbleiben. Alle angebotenen Updates sollten also zeitnah aufgespielt werden, um bekannt gewordene Sicherheitslücken sofort wieder zu schließen. Darüber hinaus kann durch Sperren von nicht benötigten Funktionen/Anwendungen die Angriffsfläche minimiert werden. Ferner kann durch restriktive Rechtevergabe (Zugriffsrechte) das Risiko gesenkt werden.

2. Implementieren Sie Fernwartungsmöglichkeiten für die Geräte, die Mitarbeiter im Homeoffice nutzen.
Regelmäßige Updates sind auch im Homeoffice ein MUSS. Darüber hinaus sollte für die

üblichen Anfragen an den betrieblichen IT-Beauftragten ein Fernzugriff auf die Endgeräte im Homeoffice eingerichtet sein. Zu diesem Zweck sollten sichere Fernwartungszugänge implementiert werden. Weiterführende Informationen des BSI zum Mobile Device Management (MDM) und zur Absicherung von Ferwartungszugängen unter diesem Link

3. Stellen Sie sicher, dass Sie Malware-Infektionen aus der Ferne erkennen können.
Außerhalb des Betriebsgebäudes sind die IT-Systeme unkalkulierbaren Risiken ausgesetzt, z.B. durch das Anschließen von USB-Sticks, die mit Malware infiziert sind. Wenn viele Mitarbeiter im Homeoffice arbeiten und von außen auf das Unternehmensnetzwerk zugreifen, sollte das Monitoring deshalb intensiviert werden. Hier spielt insbesondere die Kontrolle von Schnittstellen eine wichtige Rolle.

D. Zugriff von Mitarbeitern auf Unternehmensnetzwerk und Internet per VPN absichern
Mithilfe eines Virtual Private Networks (VPN) können zahlreiche Bedrohungen ausgeschlossen werden. Insbesondere wird das Ausspähen von Informationen durch Mitlesen des Datenverkehrs verhindert.

E. Zugriffe durch Passwort (und ggf. einen zweiten Faktor) schützen
Beim Zugriff auf das Unternehmensnetzwerk sollte stets die Berechtigung des Nutzers geprüft werden. Der Königsweg heißt hier "2-Faktor-Authentifizierung", also z.B. Passwort plus Fingerabdruck. Auch bei kurzfristigen Homeoffice-Einsätzen muss aber zumindest ein Passwortschutz implementiert sein.

F. Schatten-IT unterbinden
Wo die vom Chef genehmigten IT-Anwendungen zu langsam oder nicht anwenderfreundlich genug sind, installieren Mitarbeiter gerne ihre eigene Favoriten ("Schatten-IT"). Nicht immer genügen diese den Sicherheitsanforderungen und erhöhen damit die Risiken für das Unternehmensnetzwerk erheblich. Legen Sie daher fest, welche IT-Anwendungen für welche Arbeiten verwendet werden dürfen und welche nicht.

G. Backups machen
Erstellen Sie regelmäßig BackUps und überprüfen Sie auch ab und zu, ob Ihr Backup noch lesbar ist.

H. Mitarbeitern zusätzliche Kommunikationskanäle anbieten
Da im Homeoffice nicht „mal eben“ die Kollegin im Nachbarbüro gefragt werden kann, bietet sich die Bereitstellung zusätzlicher Kommunikationskanäle (Chatrooms oder Messenger) an.

I. Ganz spezifische Ratschläge fürs Homeoffice hat darüber hinaus der TÜV (VdTÜV) zusammengestellt:
Berufliches und Privates trennen: Wer mit dem Computer seines Arbeitgebers privat im Internet surft, kann sich auf diesem Weg gefährliche Schad-Software einfangen. Es kann daher sinnvoll sein, ein eigenes WLAN-Netzwerk für berufliche Zwecke einzurichten oder die Kommunikation der Geräte untereinander im Heimnetzwerk zu unterbinden.
Phishing-Mails löschen: Vorsicht ist derzeit bei allen E-Mails mit Bezug zum Corona-Virus geboten. Phishing-Mails enthalten Links zu gefährlichen Webseiten mit dem Ziel, Zugangsdaten des Benutzers abzufangen. Weiterhin werden gerade jetzt viele E-Mails mit Schad-Software verschickt, die nicht geöffnet werden dürfen. Nutzer sollten genau hinschauen, ob E-Mails mit Corona-Bezug von seriösen Absendern stammen. Verdächtige E-Mails sollten gelöscht oder zunächst an den IT-Support des Arbeitgebers weitergeleitet werden.
Social Engineering als Gefahr: Besonders findige Cyberkriminelle greifen Organisationen gezielt an, indem sie Mitarbeiter persönlich anschreiben und vermeintlich echte E-Mail-Adressen verwenden. Das sollten alle Beschäftigten im Hinterkopf behalten und prüfen, ob der Absender seriös oder bekannt ist.
Auf Screenshots verzichten: Derzeit machen in sozialen Netzwerken Selfies von Online-Meetings und Videokonferenzen die Runde. Ist dabei die Webadresse (URL) zu sehen, können ungebetene Gäste an den Meetings teilnehmen oder diese Informationen zur Vorbereitung von Angriffen nutzen.
Zusammenhalt dient auch der IT-Sicherheit: In schwierigen Zeiten hilft es, auch virtuell zusammenzustehen und sich digital auszutauschen. In Organisationen, die auch in der Krise viel kommunizieren, haben es kriminelle Hacker schwerer, erfolgreich zu sein oder unbemerkt zu bleiben. Rücksichtnahme, Verständnis und ein persönlicher Dank an die IT-Abteilung tun sicher allen gut.

5. Ubersicht über Sonderregeln für die Vergabe von Bauleistungen

Übersicht über Sonderregeln für die Vergabe von Bauleistungen zur Stärkung der Wirtschaft im Zusammenhang mit der Coronavirus-Pandemie.

Es wurden die in den einzelnen Bundesländern bestehenden Sonderregeln für die Vergabe von Bauleistungen zur Stärkung der Wirtschaft im Zusammenhang mit der Coronavirus-Pandemie in einer Übersicht zusammengefasst.
(cloud.bfw-suedbaden.de/index.php/s/i9aqADX6r8SFSmT)

Nicht erfasst in dieser Übersicht werden die Sonderregeln zur Beschaffung von Leistungen zur Eindämmung der Ausbreitung des neuartigen Coronavirus (sog. „Dringlichkeitsvergaben“).

6. Online-Antragstellung für Corona-Entschädigung nach § 56 Abs. 1 a Infektionsschutzgesetz

Die Online-Antragstellung für Corona-Entschädigung nach § 56 Abs. 1a Infektionsschutzgesetz ist jetzt in einigen Bundesländern möglich.
Erleiden Arbeitnehmer Verdienstausfälle aufgrund einer durch eine zuständige Stelle angeordneten Quarantäne oder eines durch die zuständige Stelle angeordneten Tätigkeitsverbotes oder erleiden sie einen Verdienstausfall, da sie durch die Betreuung ihrer Kinder aufgrund einer Schul- oder Kitaschließung nicht arbeiten können, so steht den Arbeitnehmern ein Entschädigungsanspruch nach § 56 Abs. 1 bzw. Abs.1 a Infektionsschutzgesetz (IfSG) zu. Bei Arbeitnehmern hat der Arbeitgeber für die Dauer des Arbeitsverhältnisses, längstens für sechs Wochen, die Entschädigung für die zuständige Behörde auszuzahlen. Die ausgezahlten Beträge werden dem Arbeitgeber auf Antrag von der zuständigen Behörde erstattet. Im Übrigen wird die Entschädigung von der zuständigen Behörde auf Antrag gewährt. Der Arbeitgeber kann von der zuständigen Behörde auf Antrag auch einen Vorschuss in der voraussichtlichen Höhe des Erstattungsbetrages erhalten.
Das Bundesministerium des Innern, für Bau und Heimat hat nunmehr gemeinsam mit dem nordrhein-westfälischen Ministerium für Arbeit, Gesundheit und Soziales ein Online-Verfahren entwickelt, mit dem Entschädigungsleistungen für Verdienstausfälle nach dem IfSG beantragt werden können. Das Angebot ist unter folgendem Link erreichbar: ifsg-online.de/index.html
Nach dem Stand vom 6. Mai 2020 ist lediglich das Antragsformular für Arbeitgeber für die Entschädigung nach § 56 Abs. 1a IfSG verfügbar. Erforderliche Nachweise können dem Antrag durch Upload beigefügt werden. Der Antrag wird an die zuständige Behörde (RP Freiburg) übermittelt. Es bleibt bei der Zuständigkeit der Behörden im jeweiligen Bundesland.
An dem Angebot über die Internetseite nehmen bislang acht Bundesländer teil: Brandenburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen-Anhalt und Schleswig-Holstein. Baden-Württemberg, Niedersachsen und Bremen sollen in Kürze schrittweise über die Internetseite eine Antragstellung anbieten.

VEREINIGUNG BADISCHER UNTERNEHMERVERBÄNDE E.V.
Munzinger Straße 10
79111 Freiburg
Tel.: 0761 154315-26
Fax: 0761 154315-30
E-Mail: ruff@bau-ausbau-baden.de