

Corona-Virus: Checkliste Betriebsstilllegung

Es kann passieren, dass Sie in den nächsten Wochen von einem Tag auf den anderen Ihren Betrieb schließen müssen, weil

- sich ein Mitarbeiter infiziert hat und der Betrieb unter Quarantäne gestellt wird,
- eine Ausgangssperre oder
- ein Tätigkeitsverbot für das produzierende Gewerbe verhängt wird, um das Virus einzudämmen.

Auf eine plötzliche Betriebsschließung sollten Sie vorbereitet sein:

1. **Vertretungsregelung:** Um die Kontrolle über alle Unternehmens-Prozesse zu behalten, ist es zwingend notwendig, stets Zugriff auf alle Systeme und Daten zu haben. Prüfen Sie Berechtigungskonzepte für den Datenzugriff und Vertretungsregelungen. Idealerweise gibt es für den Vertreter immer auch noch einen Stellvertreter, denn es könnten viele krank werden.
2. **Krisenstab:** Schnelle und abgestimmte Entscheidungen sind unverzichtbar in einer Krise. Richten Sie daher einen Krisenstab ein, der flexibel erreichbar ist und regelmäßig kommuniziert, um auf die volatile Situation schnell und sicher reagieren zu können. Dafür sollte der Krisenstab mit entsprechenden Vollmachten ausgestattet sein.
3. **Liquiditätsplanung** für die nächsten Wochen und Monate aufstellen. Die Kosten laufen weiter. Machen Sie eine Übersicht über alle Einnahmen und Ausgaben, bauen Sie Puffer für Verzögerungen und Ausfälle ein und überlegen Sie, wie Sie die Ausgaben runterfahren können. Parallel sollten Sie den notwendig werdenden Finanzierungsbedarf ermitteln und Hilfen bei Bank, Bund oder Landesregierung beantragen. Reden Sie mit Ihrer Bank auch über die Stundung anstehender Tilgungsraten für schon laufende Kredite. Prüfen Sie außerdem die Herabsetzung oder Stundung von Steuerzahlungen sowie fälligen Beiträgen zur BG, Sozialversicherung etc.
4. **Urlaubssperren** für zentrale Funktionen in Unternehmen prüfen und besprechen. Es muss sichergestellt sein, dass aus jeder Fachabteilung stets ein Wissensträger „im Dienst“ ist und handeln kann.
5. **Notfall-Accounts** als letzte Absicherung gegen den Ausfall von Berechtigungssystemen und Vertretungsregelungen. Für den Notfall sind diese Accounts mit klar definierten, aber erweiterten Rechten ausgestattet. Zur Sicherheit sollten die Passwörter zu einem Notfall-Account unter mehreren Mitarbeitern aufgeteilt sein. Es ist zu überlegen, ob für zentrale Prozesse (Online-Banking u.ä.) ein 4-Augen-Prinzip (also zwei Authentifizierungen) vorgesehen werden sollten. Idealerweise gibt es auch für diese Accounts eine Möglichkeit des sicheren Online-Zugriffs für den Notfall.
6. **Internetanbindung:** Verstärktes Arbeiten aus dem Homeoffice beansprucht die digitale Infrastruktur des Unternehmens. Prüfen Sie, ob die aktuelle Internetverbindung für die zahlreichen Zugriffe von außen (die Mitarbeiter im Homeoffice) ausreichende Kapazitäten bietet oder ob eine Erweiterung der Bandbreite notwendig ist.

7. **Kapazität des VPN:** In der Regel ist die Anzahl der VPN-Verbindungen – also der externen Verbindungen ins Firmennetzwerk – im Vergleich zur gesamten Belegschaft eher gering, da nur wenige Mitarbeiter aus dem Homeoffice arbeiten. Wenn alle im Homeoffice sind, wird es eng. Um das VPN zu schonen, können Sie die Mitarbeiter notfalls auffordern, das VPN nur dann zu nutzen, wenn es wirklich gebraucht wird.
8. **Telefonleitungen:** Ohne den direkten Kontakt im Büro werden vermehrt Telefonate - auch unter den Mitarbeitern - geführt. Möglicherweise muss deshalb die Zahl der Telefonleitungen erhöht oder die Mitarbeiter dazu angehalten werden, auf Mobiltelefone umzusteigen. Die Mitarbeiter könnten auch verstärkt Webkonferenzen durchführen, um die die Telefonanlage nicht weiter zu belasten. Notfalls werden nur die Sekretariate mit solchen Lizenzen ausgestattet und richten die gewünschten Konferenzen dann zentral ein.
9. **Videokonferenzen:** Für die „persönliche“ Kommunikation zwischen den Mitarbeitern oder mit Kunden oder Geschäftspartnern bieten sich Videokonferenzen an. Dafür wird allerdings bei der Internetanbindung viel Bandbreite benötigt. Ebenso muss für die richtige Software und Hardware sowie für passende Räumlichkeiten gesorgt sein.
10. **Laptops und Remotezugänge:** Voraussetzung für alle Maßnahmen ist, dass für die wichtigsten Mitarbeiter ein mobiles Gerät vorhanden, eingerichtet und auch rechtzeitig verteilt worden ist! Sollten nicht genügend Laptops vorhanden sein, können den Mitarbeitern spezielle Arbeitsumgebungen zur Verfügung gestellt werden (z.B. Teamviewer), die sie von ihren privaten Geräten nutzen können. Im Zuge einer Nutzung solcher Remotezugänge sollte die BYOD-Richtlinie („Bring-your-own-device“) geprüft und gegebenenfalls für den Ausnahmezustand angepasst werden.
11. **IT-Sicherheit:** Das Funktionieren der IT-Systeme ist jetzt von zentraler Wichtigkeit, denn persönliche Kontakte sollen vermieden werden. Kommunikation findet nun überwiegend digital statt - und dezentral, z.B. im Homeoffice der Mitarbeiter. Die Sicherheit der IT-Systeme sollte daraufhin überprüft werden. Es kann nicht ausgeschlossen werden, dass Cyberkriminelle und Hacker das allgemeine Durcheinander und die Hektik nutzen, um Sicherheitslücken auszunutzen, IT-Systeme lahm zu legen oder vermehrt Betrugs- und Erpressungsversuche zu starten. Machen Sie Ihren Mitarbeitern daher klar, dass im Homeoffice die gleichen strengen Regeln gelten wie im Betrieb (Passwortschutz etc.) und dass der Virenschutz auch auf privaten Notebooks aktuell sein muss. Eigene Software darf nur nach Rücksprache geladen und für betriebliche Zwecke genutzt werden. Warnen Sie ausdrücklich vor Schadmails, Phishing-Mails und Betrug per Social Engineering. Für den Notfall sollten BackUps jetzt nicht im Büro, sondern besser in einer Cloud liegen, auf die der IT-Administrator auch vom Homeoffice aus zugreifen kann.
12. **Telefonumleitung:** Treffen Sie Regelungen, welcher Telefonanschluss im Falle einer Betriebsschließung wohin umgeleitet wird: Jeder einzelne Anschluss auf das Handy seines Besitzers oder alle Anschlüsse zusammen auf die Zentrale - und die Zentrale auf das Handy vom Chef. Das hängt von der Betriebsgröße ab.
13. **Zutrittskontrolle:** Prüfen Sie die Zutrittsberechtigungen zum Büro (Lager etc.) daraufhin, ob ein zentrales Schließsystem vorhanden ist, das die Möglichkeit bietet, gezielt einzelnen Mitarbeitern Zugang zu gewähren und anderen zu verwehren.

14. **Posteingang:** Die Post muss weiterhin angenommen und weitergeleitet werden. Da es wenig praktikabel ist, die Sendungen direkt an die Heimatadresse weiterzuleiten, sollte hier ein Prozess definiert sein, der das Einscannen der Unterlagen und die digitale Weiterleitung abdeckt. Datenschutz und Briefgeheimnis sind zu berücksichtigen. E-Mail-Systeme können allerdings diese zusätzlichen Datenmengen oft nicht bewältigen, sodass sichere Dateiaustauschplattformen bzw. Datenräume empfohlen werden.
15. **Postversand:** Gibt es Dokumente, die unbedingt ausgedruckt werden müssen? Ist eine Unterschrift auf dem Dokument notwendig? Falls keine elektronischen Unterschriften (Signaturen) genutzt werden sollen, muss auch hier ein Prozess aufgebaut werden, um die Verarbeitung der Dokumente zu gewährleisten. Zwar ist die Einführung einer digitalen Signatur für den einzelnen Mitarbeiter relativ einfach, die Einführung elektronischer workflows benötigt dagegen einen erheblichen Vorlauf.
16. **Kurzarbeit** beantragen für nicht benötigtes (und nicht im Homeoffice befindliches) Personal (siehe ZVSL-Downloadbereich).
17. **Verdienstausfall-Entschädigung** beantragen (§ 56 InfektionsschutzG) für in Quarantäne befindliches Personal und ggf. für den Unternehmer selbst. Der Arbeitgeber muss in Quarantäne befindlichen Mitarbeitern den Verdienstausfall bezahlen und sich das Geld anschließend von den zuständigen Stellen (z.B. in NRW Landschaftsverband Rheinland bzw. Westfalen-Lippe) zurückholen.
18. **Vorräte auf Lager:** Prüfen Sie, ob wichtige Materialien und Komponenten in geeignetem Maß vorzuhalten sind, falls Lieferketten der Hersteller gestört werden.
19. **Wartungsarbeiten:** Ziehen Sie geplante Wartungsarbeiten und Verschleißteilaustausch möglichst vor. So sind Sie besser auf den Fall von Absperrungen vorbereitet, da in einem solchen Fall die notwendigen Wartungen nicht mehr möglich sind.
20. **Kommunikation mit Kunden und Lieferanten:** Stimmen Sie das weitere Vorgehen auf den Baustellen sowie fällige Zahlungen ab und halten Sie die Ergebnisse in einer Projektübersicht mit allen Baustellen fest.
21. **Kommunikation mit Mitarbeitern:** Kommunizieren Sie die geplanten Maßnahmen möglichst frühzeitig, um Unsicherheiten vorzubeugen. Sollten Sie neue Verfahren oder digitale Technik einführen, sollten Sie gründlich testen, ob sie funktioniert, und den Mitarbeitern Anleitungen zur Verfügung stellen.
22. **Notfallkoffer:** Auch der Chef kann erkranken. Für diesen Fall sollten - auch in Zeiten ohne Corona-Notfallregeln im Unternehmen bekannt sein. Vom Onlinebanking-Passwort bis zur Generalvollmacht muss alles geregelt sein, damit auch die Ehefrau oder der kaufmännische Leiter den Betrieb weiterführen können. Auf diese Daten sollte nicht nur über einen Aktenordner im Büro zugegriffen werden können, sondern auch digital vom Homeoffice aus (siehe Notfallkoffer UnternehmerINFO).
23. **Wachschutz** für Betrieb / Lagerhof / Baustellen organisieren.

24. **Kontakt halten** mit ZVSL