ALTHAMMER & KILL

Beschäftigtendatenschutz – Novelle des Infektionsschutzgesetzes

Hintergrund

In Anbetracht der kritischen Situation hat der Gesetzgeber eine deutliche Verschärfung des Infektionsschutzgesetzes beschlossen. Diese ist am 24.11.2021 in Kraft getreten. Die Entwicklungen und Interpretationen sind dynamisch, daher wird dringend empfohlen, stets die aktuelle Entwicklung im Blick zu behalten, z.B. unter https://www.bmas.de/DE/Corona/Fragen-und-Antworten/Fragen-und-Antworten-Infektionsschutzgesetz/faq-infektionsschutzgesetz.html.

Wesentliche Umsetzungs-Punkte des IfSG - ohne Anspruch auf Vollständigkeit

- Arbeitgeber müssen täglich überwachen und regelmäßig dokumentieren, ob Arbeitsstätten unter Befolgung der 3-G-Regel vom Arbeitgeber und Beschäftigten betreten werden. In vielen Betrieben wird dies sinnvollerweise durch eine Kontrolle bei Zutritt der Arbeitsstätte umgesetzt werden können, auch scheint dieses die Auffassung des Bundesministeriums für Arbeit und Soziales zu sein.
- Betreten darf die Arbeitsstätte nur, wer einen gültigen Impf- oder Genesenennachweis oder einen gültigen Testnachweis eines anerkannten Testzentrums bei sich hat oder sich im Betrieb unter Aufsicht testen lassen möchte. Die Aufsichtspersonen sind entsprechend zu unterweisen.
- Gültig ist ein Testnachweis durch anerkannte externe Teststellen bei Schnelltests 24 Stunden nach Durchführung, bei PCR-Tests 48 Stunden.
- Der Arbeitgeber muss die Einhaltung der Zugangsregel bei Ungeimpften bzw. Nicht-Genesenen täglich kontrollieren und dokumentieren.
- Bei den Genesen oder Geimpften reicht die einmalige Kontrolle und Dokumentation aus - sie sind danach von den täglichen Zugangskontrollen ausgenommen, müssen aber für den Fall behördlicher Vor-Ort-Kontrollen ihren Nachweis bei sich tragen.
- Das betriebliche Hygienekonzept sollte entsprechend überprüft und angepasst werden.
- Darüber hinaus ergeben sich arbeitsrechtliche Fragen. Diese sollten ggf. fachanwaltlich überprüft werden, unter anderem:
  - Der Arbeitgeber hat nach §4 der SARS-CoV2-Arbeitsschutzverordnung bis zum 19.03.2022 einschließlich den in Präsenz Beschäftigten 2 kostenlose Tests zur Verfügung zu stellen

- Sofern keine Nachfolgeregelung erfolgt, dürfte der Beschäftigte selbst dafür verantwortlich sein, dass er einen gültigen Nachweis besitzt, im Zweifelfall also auf eigene Kosten, wenn man die derzeit 1x wöchentlich kostenfrei durchzuführende Möglichkeit des Testens in Testzentren einmal außen vorlässt.
- Auch die Zeit für einen unter Aufsicht des Arbeitgebers durchgeführten Test könnte evtl. nicht als Arbeitszeit gelten, da das IfSG den Arbeitgeber nur zur Kontrolle und Dokumentation verpflichtet.
- Die Weigerung, einen gültigen 3G-Nachweis vorzulegen, dürfte arbeitsrechtliche Konsequenzen auslösen. Ein Anspruch ungeimpfter bzw. nicht genesener Beschäftigter auf Homeoffice lässt sich nicht aus dem IfSG ableiten.

Datenschutzrechtliche Aspekte

- Der Arbeitgeber muss die Einhaltung der 3G-Regel kontrollieren und dokumentieren. Das bedeutet, es besteht eine Verarbeitungspflicht.
- Die Daten sollten 6 Monate nach der Erhebung gelöscht werden.
- Die Beschäftigten sind nicht in der Pflicht, einen Impf- oder Genesenennachweis vorzulegen, selbst, wenn einer vorhanden sein sollte. Die Folge wäre, dass diese trotz Genesung oder Impfung tägliche Testnachweise vorweisen bzw. unter Aufsicht beim Arbeitgeber durchführen müssen.
- Indes geht die Dokumentationspflicht nicht so weit, Kopien der Nachweise anzufertigen bzw. zu dokumentieren - dieses ist weder notwendig noch erforderlich. Ähnlich wie bei Führerscheinen und Personalausweisen reicht eine Vorlage, Sichtprüfung und Bestätigung der Ordnungsmäßigkeit aus.
- Am jeweiligen Kontrolltag muss nur der Vor- und Zunamen des Beschäftigten auf einer Liste abgehakt werden, nachdem der jeweils gültige Nachweis durch den Beschäftigten erbracht worden ist.
- Bei geimpften und genesenen Personen muss das Vorhandensein eines gültigen Nachweises nur einmal erfasst und dokumentiert werden. Bei Genesenen ist zusätzlich das Enddatum des Genesenen-Status zu dokumentieren.
- Es gibt Softwarelösungen (z. B. in Form eines SaaS) für die automatische Erfassung. Hier ist die Einhaltung der datenschutzrechtlichen Regeln sowie der Informationssicherheit vorher zu prüfen, da das einsetzende Unternehmen verantwortlich ist, nicht der Anbieter der Software. Wir empfehlen, dazu vorab Kontakt mit dem Datenschutzbeauftragten aufzunehmen.

Pragmatische Durchführung der Dokumentationspflichten

Anbei wird die Erfüllung der Dokumentationspflichten mit Hilfe von Listen beispielhaft durchgespielt:

- Eine vollständige Mitarbeitenden-Liste (Vorname und Name) sollte kurzfristig von der Personalabteilung zur Verfügung gestellt werden. Die Liste kann in Papierform oder in einer Excel-Datei geführt werden, wobei angemessene Schutzmaßnahmen gegen Vernichtung, Veränderung und zur Sicherung der Vertraulichkeit gewährleistet sein müssen (wie bei Softwarelösungen selbstverständlich auch).
- Die Mitarbeitenden sollten schnellstmöglich abgefragt und gebeten werden, ihre Nachweise vorzuzeigen (z. B. physisch vor dem Beauftragten oder im Rahmen einer Videokonferenz). Es erfolgt die Erfassung:

Vorname	Name	Vorlage gültiger Impfnachweis	Vorlage gültiger Genesenennachweis	Ablaufdatum bei Genesenennachweis	Tägliche Nachweispflicht
Martin	Bosusis	nein	Ja	02.03.2022	nein
Dora	Mustermann	Ja	Nein		Nein
Heiko	Hollister	Nein	Nein		Ja
Inge	Ungefroren	Nein	Nein		Ja

- Als Folge müssen Herr Hollister und Frau Ungefroren täglich einen gültigen Testnachweis liefern, Frau Mustermann ist von der täglichen Nachweispflicht befreit, ebenso wie Herr Bosusis. Bei ihm tritt jedoch – sofern keine anderen Nachweise bis dahin vorgelegt werden - am 03.03.2022 die tägliche Nachweis- und Dokumentationspflicht wieder in Kraft.
- Für jeden Tag sollte eine neue Liste erstellt werden, dabei sind nur noch die Personen auf der Liste vorhanden, die einer täglichen Nachweispflicht unterliegen:

Datum	Vorname	Name	Vorlage gültiger Testnachweis
26.11.21	Heiko	Hollister	Ja
26.11.21	Inge	Ungefroren	Ja

- Es ist nicht gestattet, das Testergebnis selbst zu notieren. Im Falle eines positiven Testergebnisses ist in der Regel der Zugang zur Arbeitsstätte zu verweigern und es sind weitere Maßnahmen gem. betrieblichem Hygienekonzept zu ergreifen.
- Die erfassten Daten dürfen für die Anpassung des Konzeptes verwendet werden. Im Falle der Frage der Lohnfortzahlungspflicht im Ansteckungsfall bei Ungeimpften empfiehlt sich, eine erneute Erhebung im Einzelfall durchzuführen, da hier die Arbeitnehmer den Impfstatus angeben müssen.
- Die Mitarbeitenden sind über die Verarbeitung gem. Art. 13 DSGVO (bzw. den entsprechenden kirchlichen Regelungen) bei der Erhebung zu informieren.

Technische und organisatorische Schutzmaßnahmen

Egal ob eine Software-Lösung zum Einsatz kommt, Papierlisten oder Excel-Sheets - es sind zum Schutz der sensiblen Daten der Beschäftigten angemessene Schutzmaßnahmen gem. Datenschutzgrundverordnung in Verbindung mit §22 Abs. 2 Bundesdatenschutzgesetz (bzw. den entsprechenden kirchlichen Regelungen) zu treffen. Die folgende Aufzählung ist nur beispielhaft, nicht abschließend und sollte mit dem Datenschutzbeauftragten abgestimmt werden:

- Angemessenes Berechtigungs- und Sicherheitskonzept (physisch und virtuell); „Need-to-Know-Prinzip“:
- Nur berechtigte Personen einschließlich deren Vertretungen für den Urlaubs- und Krankheitsfall, dürfen Zugang zu den Daten haben. Dieses sind meistens nur sehr wenige Personen im Unternehmen.
- Der Zugang ist vor unberechtigtem Zugriff und Veränderung zu schützen, z.B. via Passwortschutz oder geschütztem Ordner/Laufwerk, Virenschutz, Patchmanagement, Firewall, 2-Faktor-Authentifizierung. Die Aufbewahrung physischer Dokumente darf nur in einem Tresor/abgeschlossenem (Metall-) Schrank mit angemessenen Schlüsselregelungen erfolgen.
- Schutz gegen Verlust, z.B. unbeabsichtigtes Löschen, in Form eines Backup-Konzepts.
- Die an der Verarbeitung Beteiligten sollten ausreichend geschult und sensibilisiert werden. Die Verpflichtung zur Vertraulichkeit sollte dokumentiert sein.
- Gesundheitsdaten sollten nicht in Clouds gespeichert werden, bei denen eine Drittlandsproblematik relevant sein könnte (z.B. Rechenzentrum in den USA).
- Physische Daten müssen nach Ablauf der gesetzlichen Aufbewahrungsfrist datenschutzkonform vernichtet (z.B. Schredder mindestens P4) und virtuelle Daten gelöscht werden (Achtung, einfaches Löschen einer Datei ist oftmals nicht ausreichend).