

Anwendungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden  
des Bundes und der Länder

---

(Stand: 20. Dezember 2021)

**Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie**

*Die nachfolgenden Ausführungen der Konferenz der unabhängigen Datenschutzbahörden des Bundes und der Länder (Datenschutzkonferenz – DSK) sollen für den praktischen Vollzug als Hilfestellung im Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) dienen.*

Die DS-GVO genießt als EU-Verordnung gemäß Artikel 288 Absatz 2 Satz 2 des Vertrags über die Arbeitsweise der Europäischen Union Anwendungsvorrang vor nationalen Gesetzen, die eine Verarbeitung personenbezogener Daten (pbD) regeln. Sie gilt für nicht-öffentliche und öffentliche Stellen unmittelbar. So können Datenverarbeitungen etwa über die allgemeinen Regelungen des Artikels 6 Absatz 1 Satz 1 DS-GVO gerechtfertigt sein.

Jedoch enthält die DS-GVO selbst keine konkreten, bereichsspezifischen Regelungen zur Verarbeitung von pbD im Beschäftigtenkontext (Beschäftigtendaten) im Pandemiefall. Stattdessen beinhalten Artikel 6 Absatz 2 und Absatz 3 DS-GVO, Artikel 9 Absatz 2 und Absatz 4 DS-GVO sowie Artikel 88 Absatz 1 DS-GVO sogenannte Öffnungsklauseln. Sie ermöglichen den Mitgliedstaaten, spezifischere Vorschriften für die Verarbeitung von Beschäftigtendaten sowie für die Verarbeitung besonderer Kategorien von pbD im Sinne von Artikel 9 Absatz 1 DS-GVO (Gesundheitsdaten) zu erlassen. Der Bundesgesetzgeber hat zum Beispiel mit Datenverarbeitungsregelungen im Infektionsschutzgesetz (IfSG) sowie der Landesgesetzgeber mit ergänzenden Verordnungen zur Corona-Pandemie von den Öffnungsklauseln Gebrauch gemacht.

Die DSK hat bereits mit Pressemitteilung vom 13. März 2020 über rechtliche Vorgaben im Hinblick auf die Verarbeitung von personenbezogenen Daten durch Arbeitgeberinnen und Arbeitgeber sowie Dienstherren im Zusammenhang mit der Corona-Pandemie informiert.

Die Pressemitteilung der DSK finden Sie hier:

[https://www.datenschutzkonferenz-online.de/media/pm/20200325\\_Informationen\\_zu\\_Corona\\_und\\_Arbeitgeber.pdf](https://www.datenschutzkonferenz-online.de/media/pm/20200325_Informationen_zu_Corona_und_Arbeitgeber.pdf)

Ferner hat sie in ihrer EntschlieÙung vom 3. April 2020 „Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie“ auf die grundlegenden Vorgaben der DS-GVO hingewiesen. Diese sind auch im Pandemiefall bei der Verarbeitung von Beschäftigtendaten und Gesundheitsdaten zu beachten.

In Ergänzung dazu hat die DSK in ihrer EntschlieÙung vom 29. März 2021 „Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!“ verdeutlicht, dass es an normenklaren Regelungen zu Datenverarbeitungen im Pandemiefall mangelt. In diesem Zusammenhang wurde der Gesetzgeber aufgefordert, entsprechende Gesetzgebungsverfahren in die Wege zu leiten, um Rechtsklarheit, Rechtssicherheit und einheitliche Lösungen zu erreichen.

Die EntschlieÙungen der DSK finden Sie hier:

<https://www.datenschutzkonferenz-online.de/entschliessungen.html>

Die DSK nimmt mit dem vorliegenden Papier zu den sich aus der praktischen Arbeit ergebenden Fragen Stellung. Hierdurch soll eine bundesweite und länderübergreifende Rechtsanwendung bei der Pandemiebekämpfung im Bereich des Beschäftigtendatenschutzes vereinfacht werden. Die folgenden Fallgestaltungen beziehen sich auf die Verarbeitung von Daten der Beschäftigten, einschließlich von deren Gesundheitsdaten, durch Arbeitgeberinnen und Arbeitgeber. Die Ausführungen gelten auch für Beschäftigte im öffentlichen Bereich, soweit für diese nicht besondere Regelungen vorrangig anzuwenden sind.

## **Inhaltsverzeichnis**

<b>1. Dürfen Beschäftigtendaten zur Pandemiebekämpfung verarbeitet werden?</b> .....	<b>1</b>
<b>2. Dürfen Beschäftigtendaten mittels eines „Kontakt-Tagebuches“ (berufsbedingte beziehungsweise innerbetriebliche Kontakte) zur Pandemiebekämpfung verarbeitet werden? .....</b>	<b>3</b>
<b>3. Dürfen private Kontaktdaten der Beschäftigten zur Pandemiebekämpfung verarbeitet werden? .....</b>	<b>4</b>
<b>4. Dürfen positiv getestete Beschäftigte innerhalb der gesamten Belegschaft oder gegenüber ihren (möglichen) Kontaktpersonen namentlich bekannt gegeben werden? .....</b>	<b>5</b>
<b>5. Dürfen zur Befreiung der Beschäftigten von der Pflicht zum Tragen einer Mund-Nase-Bedeckung (MNB) ärztliche Bescheinigungen mit konkreten Gesundheitsangaben verarbeitet werden? .....</b>	<b>6</b>
<b>6. Dürfen Beschäftigtendaten mittels Einsatz von sogenannten Wärmebildkameras zur Pandemiebekämpfung verarbeitet werden? .....</b>	<b>7</b>
<b>7. Dürfen Beschäftigtendaten bei der Nutzung von Videokonferenzsystemen verarbeitet werden? .....</b>	<b>8</b>
<b>8. Dürfen Arbeitgeberinnen und Arbeitgeber die „3-G-Daten“ ihrer Beschäftigten verarbeiten? .....</b>	<b>8</b>
<b>9. Dürfen Arbeitgeberinnen und Arbeitgeber für ihre Beschäftigten Impftermine organisieren und in diesem Zusammenhang pbD verarbeiten?.....</b>	<b>17</b>

## 1. Dürfen Beschäftigtendaten zur Pandemiebekämpfung verarbeitet werden?

### Antwort:

Ja, in sehr engen Grenzen.

Zwar ist es datenschutzrechtlich grundsätzlich nicht vorgesehen, dass Arbeitgeberinnen und Arbeitgeber als Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO für den Zweck „Pandemiebekämpfung“ Beschäftigtendaten verarbeiten. Die Pandemiebekämpfung sowie die Entscheidung über die eingesetzten Mittel sind Aufgaben des Staates. Arbeitgeberinnen und Arbeitgeber dürfen jedoch begrenzt Beschäftigtendaten im Zusammenhang mit der Pandemiebekämpfung verarbeiten. Hierfür gelten die nachfolgenden allgemeinen Grundsätze (siehe auch die Pressemitteilung der DSK vom 13. März 2020, diese finden Sie hier: <https://www.datenschutzkonferenz-online.de/pressemitteilungen.html>):

Die Berechtigung zur Verarbeitung von Beschäftigtendaten ergibt sich für Arbeitgeberinnen und Arbeitgeber aus dem nicht-öffentlichen Bereich aus § 26 Absatz 1 Bundesdatenschutzgesetz (BDSG) beziehungsweise Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO jeweils in Verbindung mit den tarif-, arbeits- und sozialrechtlichen Regelungen des nationalen Rechts. Soweit Gesundheitsdaten verarbeitet werden, sind zudem spezialgesetzliche Bestimmungen, wie die des IfSG sowie § 26 Absatz 3 BDSG und Artikel 9 Absatz 2 Buchstabe b DS-GVO einschlägig.

Bei Maßnahmen gegenüber Dritten kann Artikel 6 Absatz 1 Buchstabe f DS-GVO als Rechtsgrundlage herangezogen werden. Soweit besonders sensible Daten – wie Gesundheitsdaten – betroffen sind, findet zudem Artikel 9 Absatz 2 Buchstabe i in Verbindung mit § 22 Absatz 1 Nummer 1 Buchstabe c BDSG Anwendung.

Die Fürsorgepflicht der Arbeitgeberinnen und Arbeitgeber verpflichtet diese, den Gesundheitsschutz der Gesamtheit ihrer Beschäftigten sicherzustellen. Hierzu zählt nach Ansicht der unabhängigen Datenschutzaufsichtsbehörden auch die angemessene Reaktion auf die epidemische beziehungsweise pandemische Verbreitung einer meldepflichtigen Krankheit, die insbesondere der Vorsorge und im Fall der Fälle der Nachverfolgbarkeit (also im Grunde nachgelagerte Vorsorge gegenüber den Kontaktpersonen) dient. Diese Maßnahmen müssen dabei auch verhältnismäßig sein. Die Daten sind vertraulich zu behandeln und dürfen ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks (regelmäßig also spätestens am Ende der Pandemie) müssen die erhobenen Daten unverzüglich gelöscht werden.

Eine Einwilligung der von den Maßnahmen Betroffenen allein sollte hingegen vorliegend nur als datenschutzrechtliche Verarbeitungsgrundlage in Betracht gezogen werden, wenn die Betroffenen über die Datenverarbeitung informiert sind, freiwillig in die Maßnahme einwilligen können und dabei den Anforderungen des § 26 Absatz 2 Satz 2 BDSG Rechnung getragen wird. Die Wertung des BDSG findet auch auf Beschäftigte im öffentlichen Bereich Anwendung.

Weitere Ausführungen zu den Hinweis- und Informationspflichten aus Artikel 12, 13 und 14 DS-GVO finden Sie im Kurzpapier Nummer 10 der DSK „Informationspflichten bei Dritt- und Direkterhebung“.

Dieses ist hier veröffentlicht:

[https://www.datenschutzkonferenz-online.de/media/kp/dsk\\_kpnr\\_10.pdf](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf).

Weitergehende Hinweise zu den einzelnen Voraussetzungen einer wirksamen Einwilligung enthalten die Leitlinien Nummer 05/2020 des Europäischen Datenschutzausschusses vom 4. Mai 2020 sowie das Kurzpapier Nummer 20 „Einwilligung nach der DS-GVO“ der DSK.

Diese finden sie hier:

[Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 | European Data Protection Board \(europa.eu\)](#)

[https://www.datenschutzkonferenz-online.de/media/kp/dsk\\_kpnr\\_20.pdf](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf)

In diesem Zusammenhang ist bei Beschäftigten auch zu beachten, dass die Einwilligung zweckgebunden sowie grundsätzlich schriftlich oder elektronisch zu erfolgen hat, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist, § 26 Absatz 2 Satz 3 BDSG.

Weiter müssen auch im Zusammenhang mittels einer Einwilligung verarbeiteten Gesundheitsdaten angemessene und spezifische Schutzmaßnahmen getroffen werden, § 26 Absatz 3 Satz 3 in Verbindung mit § 22 Absatz 2 BDSG.

Zusätzlich zu den bestehenden Rechtsgrundlagen für die Datenverarbeitung auf Seiten der Arbeitgeberinnen und Arbeitgeber ergeben sich aus dem Tarifrecht beziehungsweise dem Arbeitsrecht für Beschäftigte verschiedene Nebenpflichten, unter anderem auch Rücksichts-, Verhaltens- und Mitwirkungspflichten gegenüber ihren Arbeitgeberinnen und Arbeitgebern sowie Dritten.

## **2. Dürfen Beschäftigtendaten mittels eines „Kontakt-Tagebuches“ (berufsbedingte beziehungsweise innerbetriebliche Kontakte) zur Pandemiebekämpfung verarbeitet werden?**

### **Antwort:**

Grundsätzlich ja.

Weisen Arbeitgeberinnen und Arbeitgeber Beschäftigte an, ein Kontakttagebuch zu führen, sind sie für die in diesem Rahmen erfolgende Verarbeitung von pbD Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO.

Die Pandemiebekämpfung<sup>1</sup> ist zumindest ein berechtigtes Interesse von Arbeitgeberinnen und Arbeitgebern. Der Pandemiebekämpfung dient unter anderem dazu, dass Arbeitgeberinnen und Arbeitgeber nach der Information einer oder eines Beschäftigten, an COVID-19 erkrankt zu sein, deren oder dessen berufsbedingte beziehungsweise innerbetriebliche Kontakte versuchen zu ermitteln, diese über die Risikobegegnung unterrichten und gegebenenfalls innerbetriebliche Vorkehrungen treffen können (zum Beispiel „Homeoffice, Einzelbüro, Freistellung zur Testung). An dieser Stelle überwiegen die berechtigten Interessen der Arbeitgeberinnen und Arbeitgeber das Recht auf informationelle Selbstbestimmung der Beschäftigten (Artikel 6 Absatz 1 Buchstabe f DS-GVO, siehe Antwort zur Frage 1).

Anderes gilt allerdings für Kontakt-Historie-Daten, die von Beschäftigte erfasst werden sollen, deren Berufsausübung einem gesetzlich angeordneten besonderen Geheimnisschutz unterliegt, etwa für die betrieblichen Datenschutzbeauftragten, Betriebsratsmitglieder oder im Betrieb angestellte Betriebsärzte oder Betriebsärztinnen. Soweit in diesen Fällen ein Kontakt-Tagebuch den Geheimnisschutz ihrer Kontaktpersonen verletzen würde, überwiegen die schutzwürdigen Interessen der Betroffenen beziehungsweise fehlt es grundsätzlich an einem spezifischen gesetzlichen Erlaubnistatbestand zur Durchbrechung des Berufsgeheimnisschutzes. Eine Herausgabe beziehungsweise Übermittlung der Kontaktdaten an Arbeitgeberinnen oder Arbeitgeber ist in diesen Fällen unzulässig.

Jedoch kann im Rahmen einer Ermittlungstätigkeit des Gesundheitsamtes nach § 25 IfSG die Offenlegung der Kontaktdaten gegenüber (nur) diesem zulässig sein, wenn es anlässlich einer dem Geheimschutz unterliegenden Tätigkeit zu

---

<sup>1</sup> Hinter dem Interesse an der Pandemiebekämpfung steht das berechtigte Interesse des Arbeitgebers oder der Arbeitgeberin, das Ansteckungsrisiko in seinem oder ihrem Unternehmen zu reduzieren beziehungsweise schnell eingrenzen zu können, um so auch den Betrieb seines oder ihres Unternehmens unter den Bedingungen der Pandemie soweit wie möglich aufrechtzuerhalten.

einer Ansteckung mit dem Coronavirus SARS-CoV-2 gekommen ist. Die Verschwiegenheitspflicht steht der Offenlegung der Kontaktdaten dann nicht entgegen.

Im Zusammenhang mit dem Führen von Kontakt-Tagebüchern ist zu beachten:

- Grundsatz der „Zweckbindung“, Artikel 5 Absatz 1 Buchstabe b DS-GVO: Grundsätzlich dürfen Arbeitgeberinnen und Arbeitgeber die Eintragungen in einem Kontakt-Tagebuch nur dann nutzen, wenn ein Infektionsfall vorliegt;
- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Es dürfen nur die für die Kontaktnachverfolgung notwendigen pbD erfasst werden. Die Nutzung der Kontaktdaten ist auf einen möglichst engen Kreis spezifisch ermächtigter Personen zu beschränken; dabei darf auf die Eintragungen aus einem Kontakt-Tagebuch in der Regel nicht direkt zugegriffen werden – es ist ausreichend, wenn die Kontakte genannt werden;
- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e DS-GVO, Recht auf Löschung, Artikel 17 DS-GVO: Soweit durch besondere Regelungen keine anderen Speicherfristen festgelegt sind, dürfen Eintragungen regelmäßig nicht länger als zwei Wochen nach dem Kontakt gespeichert und sollten nach einer gegebenenfalls erfolgten Mitteilung an Arbeitgeberinnen und Arbeitgeber gelöscht werden (Zweckerfüllung);
- Grundsätze der „Integrität und Vertraulichkeit“, Artikel 5 Absatz 1 Buchstabe f DS-GVO und deren Gewährleistung, Artikel 24, 25 und 32 DS-GVO: Das Kontakt-Tagebuch muss vor dem Zugriff Unbefugter geschützt sein.

### **3. Dürfen private Kontaktdaten der Beschäftigten zur Pandemiebekämpfung verarbeitet werden?**

**Antwort:**

Ja, zumindest wenn eine wirksame Einwilligung der Beschäftigten vorliegt.

Grundsätzlich haben Arbeitgeberinnen und Arbeitgeber keinen Anspruch darauf, dass Beschäftigte ihre privaten Telefonnummern und / oder E-Mail-Adressen für betriebliche Zwecke angeben. Möchte der Arbeitgeber oder die Arbeitgeberin private Erreichbarkeitsdaten der Beschäftigten erhalten, um im Falle einer Infektion eines oder einer Beschäftigten an dessen oder deren Kontaktpersonen heranzutreten und letztere über die Risikobegegnung zu unterrichten, setzt das die Einwilligung der betroffenen Beschäftigten voraus. Die Einwilligung muss freiwillig erteilt werden. Wegen des zwischen Arbeitgeberinnen und Arbeitgebern sowie Beschäftigten bestehenden Über- und Unterordnungsverhältnisses

wird regelmäßig die Freiwilligkeit einer Einwilligung bei Beschäftigten nicht gegeben sein. In § 26 Absatz 2 Satz 2 BDSG hat der Gesetzgeber jedoch beispielhaft Indizien genannt, wann bei Beschäftigten die Freiwilligkeit ihrer Einwilligung ausnahmsweise angenommen werden könnte: wenn für diese ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeberinnen und Arbeitgeber sowie die Beschäftigten gleichgelagerte Interessen verfolgen. Die Nutzung der privaten Kontaktdaten dient hier der Pandemiebekämpfung<sup>2</sup>. Somit werden sowohl Interessen der Arbeitgeberinnen und Arbeitgeber als auch der Beschäftigten verfolgt. Es liegen grundsätzlich gleichgelagerte Interessen vor, so dass an dieser Stelle die Freiwilligkeit der Einwilligung angenommen werden kann. Dabei muss allerdings durch geeignete Maßnahmen gewährleistet sein, dass die Erteilung etwaiger Einwilligungen tatsächlich freiwillig, zweckgebunden sowie schriftlich oder elektronisch erfolgt. Zur Einwilligung siehe auch Ausführungen unter Frage 1.

Zu beachten ist weiter, dass Arbeitgeberinnen und Arbeitgeber die privaten Kontaktdaten nur zweckgebunden – das bedeutet hier nur für die Pandemiebekämpfung – verarbeiten dürfen.

#### **4. Dürfen positiv getestete Beschäftigte innerhalb der gesamten Belegschaft oder gegenüber ihren (möglichen) Kontaktpersonen namentlich bekannt gegeben werden?**

**Antwort:**

Grundsätzlich nein.

Die namentliche Bekanntgabe der positiv getesteten Beschäftigten innerhalb der gesamten Belegschaft ist zur Wahrnehmung des vom Arbeitgeber oder der Arbeitgeberin verfolgten Interesses nicht erforderlich; in aller Regel gilt dies auch für eine Bekanntgabe gegenüber ihren (möglichen) Kontaktpersonen unter den Beschäftigten. Die einzelnen Kontakte können bei der oder dem erkrankten Beschäftigten abgefragt und im Anschluss – ohne deren oder dessen Namensnennung – über eine mögliche Infektion informiert werden.

---

<sup>2</sup> Zu der Erläuterung des Begriffs siehe Fußnote 1.



## 5. Dürfen zur Befreiung der Beschäftigten von der Pflicht zum Tragen einer Mund-Nase-Bedeckung (MNB) ärztliche Bescheinigungen mit konkreten Gesundheitsangaben verarbeitet werden?

### Antwort:

Nein, nur in Ausnahmefällen.

Beschäftigte können in Betriebsstätten zum Tragen einer MNB verpflichtet sein. Landesrechtliche Rechtsvorschriften zur Pandemiebekämpfung lassen hiervon Ausnahmen aus gesundheitlichen Gründen zu. Hierzu müssen die Beschäftigten ihren Arbeitgeberinnen und Arbeitgebern als Nachweis in der Regel ein ärztliches Attest oder eine vergleichbare Bescheinigung zur Glaubhaftmachung der Befreiungsvoraussetzungen vorlegen. Die landesrechtlichen Vorschriften enthalten dabei regelmäßig weitere und teils unterschiedliche Anforderungen, die ein solcher Nachweis erfüllen muss.

Bei der Antwort auf die Frage, ob ein Nachweis detaillierte Gesundheitsdaten der Beschäftigten, wie etwa Angaben zu Vorerkrankungen, enthalten muss, spielen somit zunächst die jeweils einschlägigen landesrechtlichen Vorgaben sowie bereits ergangene gerichtliche Entscheidungen eine wesentliche Rolle.

Spezifische Hilfestellungen hierzu erhalten Sie durch die für Sie jeweils zuständige Datenschutz-Aufsichtsbehörde.

In diesem Zusammenhang gibt die DSK Folgendes zu bedenken: Es könnte für arbeitsrechtliche Maßnahmen, wie etwa Kündigungen aus gesundheitlichen Gründen – je nach Vorerkrankung – bereits ausreichen, dass Arbeitgeberinnen und Arbeitgeber von diesen erfahren. Damit könnte die Vorlage von ärztlichen Attesten oder vergleichbarer Bescheinigungen, die detaillierte Gesundheitsdaten enthalten, für Beschäftigte – im Einzelfall – weitreichende Folgen haben; und dies weit über die Pandemie hinaus.

Werden Verantwortlichen durch Beschäftigte ärztliche Atteste oder vergleichbare Bescheinigungen mit oder ohne detaillierte Gesundheitsdaten vorgelegt, ist weiter Folgendes zu beachten:

- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Die Atteste beziehungsweise vergleichbare Bescheinigungen dürfen weder im Original noch in Kopie in die Personalakte aufgenommen werden. Es ist ausreichend, wenn in der betreffenden Personalakte vermerkt wird, dass diese jeweils vorgelegt worden sind;

- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e, Recht auf Löschung, Artikel 17 DS-GVO:  
Entfällt die Pflicht zum Tragen einer MNB, sind die pbD über die Befreiung zu löschen.

## **6. Dürfen Beschäftigtendaten mittels Einsatz von sogenannten Wärmebildkameras zur Pandemiebekämpfung verarbeitet werden?**

### **Antwort:**

Grundsätzlich Nein.

Detailliertere Ausführungen finden Sie in dem Beschluss der DSK mit dem Titel „Einsatz von Wärmebildkameras beziehungsweise elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie“.

Diesen finden Sie hier: [https://www.datenschutzkonferenz-online.de/media/dskb/20200910\\_beschluss\\_waerembildkameras.pdf](https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waerembildkameras.pdf).

Ausnahmsweise wäre die Temperaturmessung mittels Wärmebildkameras, zum Beispiel am Betriebseingang, dann erlaubt, wenn die Beschäftigten hierin wirksam einwilligen. An die Wirksamkeit einer Einwilligung sind jedoch hohe Voraussetzungen geknüpft, siehe hierzu auch Ausführungen unter Frage 1. Unter anderem kann die Freiwilligkeit einer Einwilligung vorliegen, wenn Arbeitgeberinnen und Arbeitgeber sowie Beschäftigte gleichgelagerte Interessen verfolgen, § 26 Absatz 2 Satz 2 BDSG.

Der Einsatz von Wärmebildkameras dient der Pandemiebekämpfung. Diese liegt sowohl im Interesse der Arbeitgeberinnen und Arbeitgeber als auch im Interesse der Beschäftigten. Damit liegen grundsätzlich gleichgelagerte Interessen vor. Haben die Beschäftigten aber keine Wahl, weil sie zum Beispiel alle den mit einer Wärmebildkamera ausgestatteten Betriebseingang nutzen müssen, dann kann keine Freiwilligkeit der Einwilligung angenommen werden. Sind mehrere Betriebseingänge vorhanden, darunter auch solche ohne eine Wärmebildkamera, besteht für die Beschäftigten eine Wahlmöglichkeit. Bei einer derart bestehenden Wahlmöglichkeit erscheint es möglich, die Datenverarbeitungen auf eine Einwilligung zu stützen.

Wird die Verarbeitung der Körpertemperatur auf eine Einwilligung des Beschäftigten gestützt, muss sich die Einwilligung ausdrücklich auf dieses Datum beziehen, § 26 Absatz 3 Satz 2 BDSG.

## 7. Dürfen Beschäftigtendaten bei der Nutzung von Videokonferenzsystemen verarbeitet werden?

### Antwort:

Grundsätzlich Ja.

Allerdings ist eine dauerhafte Kameraüberwachung im „Homeoffice“ unzulässig.

Weitere Ausführungen finden Sie in den Veröffentlichungen der DSK zu diesem Thema. Diese finden Sie hier:

- Orientierungshilfe Videokonferenzsysteme, Stand 23. Oktober 2020, siehe insbesondere die Ausführungen unter Nummer 3.4
- Checkliste Datenschutz in Videokonferenzsystemen (bezogen auf die Orientierungshilfe Videokonferenzsysteme, Stand 23. Oktober 2020), Stand 11. November 2020

Beide Veröffentlichungen finden Sie hier:

<https://www.datenschutzkonferenz-online.de/orientierungshilfen.html>.

## 8. Dürfen Arbeitgeberinnen und Arbeitgeber die „3-G-Daten“ ihrer Beschäftigten verarbeiten?

### Antwort:

Ja, aber nur in gesetzlich geregelten Fällen:

- **Zutrittskontrolle zur Arbeitsstätte; § 28b Absatz 1 Satz Variante 1, Absatz 3 IfSG**

Vorab weist die DSK darauf hin, dass der Wortlaut des § 28b IfSG auslegungsbedürftig ist und erheblichen Auslegungsspielraum zulässt. Der Gesetzgeber wird an dieser Stelle aufgefordert, mit einer Gesetzesänderung eine normenklare Regelung zu schaffen. Im Folgenden werden zu den einzelnen, durch § 28b IfSG eröffneten, Verarbeitungsmöglichkeiten diejenigen dargestellt, die dem Grundsatz der Datensparsamkeit am ehesten entsprechen.

Kann an einer Arbeitsstätte ein Zusammentreffen mit anderen Personen nicht ausgeschlossen werden, dürfen Arbeitgeberinnen und Arbeitgeber sowie ihre Beschäftigten die Arbeitsstätte nur betreten, wenn sie

- gegen das Coronavirus SARS-CoV-2 geimpft (§ 2 Nummer 2 COVID-19-Schutzmaßnahmen-Ausnahmenverordnung (SchAusnahmV),

- von einer Infektion mit dem Coronavirus SARS-CoV-2 genesen (§ 2 Nummer 4 SchAusnahmV) oder
- auf eine Infektion mit dem Coronavirus SARS-CoV-2 negativ getestet sind (§ 2 Nummer 6 SchAusnahmV, § 28b Absatz 1 Satz 2 IfSG) (im Folgenden geimpft, genesen, getestet)

und

- einen jeweiligen Nachweis darüber mit sich führen,
- zur Kontrolle bereithalten oder
- bei ihrer Arbeitgeberin oder ihrem Arbeitgeber hinterlegt haben (§ 28b Absatz 1 IfSG).

Was im Einzelnen als Arbeitsstätte gilt, lässt sich anhand des § 2 Absatz 1 und 2 der Arbeitsstättenverordnung beurteilen. Beispiele sind: Arbeitsräume oder andere Orte in Gebäuden oder im Freien auf dem Gelände eines Betriebs, aber auch auf Baustellen.

Wer im Einzelnen als Beschäftigter im Sinne des IfSG § 28b Absatz 1 IfSG gilt, ist § 2 Absatz 2 des Arbeitsschutzgesetzes (ArbSchG) zu entnehmen.

Arbeitgeber und Arbeitgeberinnen sind nach § 28b Absatz 3 Satz 1 IfSG verpflichtet zu prüfen, ob Beschäftigte, die ihre Arbeitsstätte betreten, geimpft, genesen oder aber getestet sind (Überprüfungspflicht).

Da letztlich nur von Bedeutung ist, dass vor Betreten der Arbeitsstätte durch den jeweiligen Beschäftigten ein gültiger 3G-Nachweis vorgelegt wurde, wird der Überprüfungspflicht ausreichend entsprochen, wenn das vorgelegte Dokument durch die Arbeitgeberin oder den Arbeitgeber gesichtet beziehungsweise auf seine Gültigkeit hin überprüft wird (§ 2 Nummer 3, 5 und 7 SchAusnahmV).

Arbeitgeberinnen und Arbeitgeber dürfen für die Erfüllung ihrer Überprüfungspflicht eigene Beschäftigte einsetzen oder Dritte beauftragen. Dabei ist zu beachten, dass – je nach Umfang der Datenverarbeitung durch die Dritten – möglicherweise Arbeitgeberinnen und Arbeitgeber mit diesen einen Auftragsverarbeitungsvertrag schließen müssen (Artikel 28 DS-GVO). Dritte sollten zur Verschwiegenheit verpflichtet, die eigenen Beschäftigten in diesem Zusammenhang auf ihre – auch innerbetrieblich geltende – Verschwiegenheitspflicht sensibilisiert werden.

- Kontrolle am „Werkstor“ durch Pfortendienst

In Fällen, in denen die Kontrolle der Beschäftigten „am Werkstor“ zum Beispiel durch einen Pfortendienst erfolgt, ist sichergestellt, dass nur kontrollierte Beschäftigte Zutritt zur Arbeitsstätte erlangen. Dabei reicht es aus, dass die Beschäftigten einen 3G-Nachweis vorlegen. Nach dem Gesetzeswortlaut ist die Frage offen, ob ein Abgleich des vorgelegten 3G-Nachweises mit Ausweisdokumenten erforderlich ist. An dieser Stelle müsste das Gesetz normenklar geändert werden. Praxisüblich dürfte – bei den kontrollierenden Personen nicht persönlich bekannten Beschäftigten – ein Sichtabgleich des 3G-Nachweises mit einem Werksausweis sein. In den Fällen, in denen kein Werksausweis existiert, könnte der Sichtabgleich des 3G-Nachweis mit einem amtlichen Ausweisdokument erfolgen.

- CovCheckPass-App

Legen Beschäftigte ihren 3G-Nachweis in digitaler Form vor, besteht auch für Arbeitgeberinnen und Arbeitgeber sowie die durch sie beauftragten Dritten die Möglichkeit, die Gültigkeit dieses Nachweises digital zu überprüfen: Arbeitgeberinnen und Arbeitgeber sowie die durch sie beauftragten Dritten können hierfür auf betriebseigenen Geräten zum Beispiel kostenfrei die CovCheckPass-App des Robert Koch-Instituts (RKI) (<https://www.digitaler-impfnachweis-app.de/covpasscheck-app/>) installieren und mit dieser datensparsam die Gültigkeit des 3G-Nachweises im Einzelfall prüfen. Die überprüfende Person sieht lediglich, dass ein gültiges Zertifikat vorliegt, nicht aber ob sich zum Beispiel um ein Impf- oder Genesenzertifikat handelt. Weiterhin wird der Nachname, Vorname und das Geburtsdatum zur Verifizierung angezeigt. Ist der überprüfte Beschäftigte der kontrollierenden Person nicht persönlich bekannt, wird zudem – wie eben dargestellt – ein Sichtabgleich des 3G-Nachweises mit einem Werksausweis und wenn dieser nicht existiert mit einem amtlichen Ausweisdokument erforderlich sein. Eine Speicherung der digital durch den Beschäftigten vorgezeigten Daten findet durch die CovCheckPass-App nicht statt. Setzen Arbeitgeberinnen und Arbeitgeber sowie durch sie beauftragte Dritte zur Erfüllung ihrer Überprüfungspflicht digitale Anwendungen ein, bleiben sie für die datenschutzkonforme Verarbeitung der Beschäftigtendaten weiterhin verantwortlich (Artikel 4 Nummer 7 DS-GVO).

- Vereinfachte Kontrollprozesse

In der Gesetzesbegründung zu dieser Vorschrift wird ausgeführt, dass „bei den Kontrollen der Nachweise über den Status geimpft und genesen [...] vereinfachte Kontrollprozesse anwendbar“ seien. Der Schwerpunkt

der Kontrollen soll auf dem tagesaktuellen Testnachweis der Beschäftigten liegen (vergleiche Deutscher Bundestag, 20. Wahlperiode, Drucksache 20/89, dort Seite 18, unter: <https://dserver.bundestag.de/btd/20/000/2000089.pdf>). Aus dem Wortlaut der Vorschrift selbst ergibt sich jedoch nicht, dass Arbeitgeberinnen oder Arbeitgeber sowie die durch sie beauftragte Dritte differenziert erfassen dürfen, ob Beschäftigte geimpft, genesen oder getestet sind. Ist dies tatsächlich durch den Gesetzgeber gewünscht, müsste dies in der Vorschrift mit einer Gesetzesänderung normenklar geregelt werden. Möchten nun Arbeitgeberinnen und Arbeitgeber für einen vereinfachten Kontrollprozess den 2G-Status ihrer Beschäftigten und gegebenenfalls das Enddatum des jeweiligen Status (zum Beispiel bei Genesenennachweisen, digitalen Nachweisen) erfassen, wird ihnen aus Gründen der Rechtssicherheit geraten, die Einwilligung ihrer Beschäftigten einzuholen. Zu den Anforderungen an eine freiwillige und damit rechtswirksame Einwilligung siehe Antwort unter 1. Für diese Rechtsauffassung spricht auch, dass Beschäftigte nicht verpflichtet sind, einen bestimmten 3G-Nachweis zu erbringen. Es ist genesenen oder geimpften Beschäftigten weiterhin freigestellt, auch aktuelle Testnachweise anstelle von Impf- oder Genesenennachweisen mitzuführen und bei Zutrittskontrollen ihrer Arbeitgeberin oder ihres Arbeitgebers vorzulegen. Die Überprüfungspflicht der Arbeitgeberinnen und Arbeitgeber über den 3G-Status ihrer Beschäftigten ist – nach dem Wortlaut des Gesetzes – nicht mit einem umfänglichen Fragebogen über den Impf- oder Genesungsstatus verbunden.

Bei den Geimpften/Genesenen können mit ihrer jeweiligen Einwilligung folgende Daten verarbeitet werden: Zutrittsdatum, Vor- und Zuname, Tatsache, dass ein 2G-Nachweis vorgelegt worden ist, gegebenenfalls Ablaufdatum.

Beispiel:

Zutrittsdatum	Vorname	Zuname	2G-Nachweis vorgelegt	(gegebenenfalls) Ablaufdatum
01.12.2021	Max	Müller	+/-Haken o. Ä.	

Die Erfassung weiterer Daten, wie zum Beispiel Impfmittel, oder gar die Kopie sowie die Speicherung des Impfnachweises und/oder Genesenennachweises selbst ist nicht erforderlich.

Mit Einwilligung der betroffenen Beschäftigten können Arbeitgeberinnen und Arbeitgeber deren Impf- oder Genesenennachweise hinterlegen. Dabei ist die Hinterlegung eine durch den Beschäftigten zu wählende, nicht verpflichtende Option.

- Vorabübermittlung eines 3G-Nachweises

Es ist gesetzlich nicht vorgesehen, dass 3G-Nachweise bereits vorab postalisch oder elektronisch (beispielsweise per E-Mail oder in einer Videokonferenz) an Arbeitgeberinnen und Arbeitgeber übermittelt werden. Eine solche Möglichkeit kann Beschäftigten regelmäßig nur auf Grundlage einer freiwilligen und damit rechtswirksamen Einwilligung eröffnet werden. Willigt der Beschäftigte nicht in die Vorabübermittlung seines 3G-Nachweises ein, muss ihm die Möglichkeit gegeben werden, vor Betreten der Arbeitsstätte seinen 3G-Nachweis vorzeigen zu können. Falls Arbeitgeberinnen und Arbeitgeber Beschäftigten in diesem Zusammenhang anbieten, den 3G-Nachweis elektronisch einzureichen, müssen sie geeignete und angemessene Verfahren vorhalten, um Vertraulichkeit und Integrität der übertragenen Daten zu wahren (zum Beispiel obligatorische Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung von E-Mails).

- Durch Arbeitgeberinnen und Arbeitgeber angebotene Tests

Es gibt drei Arten, wie Beschäftigte ein Testnachweis gegenüber Arbeitgeberinnen und Arbeitgebern erbringen können:

- mittels einer Testbescheinigung eines zugelassenen Testzentrums, einer Apotheke oder einer Ärztin/eines Arztes;
- sofern durch Arbeitgeberinnen und Arbeitgeber angeboten, mittels einer betrieblichen Testung durch Personal, das die dafür erforderliche Ausbildung oder Kenntnis und Erfahrung besitzt, zum Beispiel Betriebsärzte;
- sofern durch Arbeitgeberinnen und Arbeitgeber angeboten, mittels Durchführung eines Selbsttests unter Aufsicht.

Hinsichtlich der ersten Variante (Testnachweis mittels Testbescheinigung) wird auf die obigen Ausführungen betreffend die 3G-Nachweise verwiesen.

Bei den beiden durch Arbeitgeberinnen und Arbeitgeber möglicherweise angebotenen Nachweisvarianten ist zu beachten, dass im Anschluss an negative Testergebnisse keine weitere Verarbeitung von Beschäftigten-daten erforderlich sein dürfte. Fällt die betriebliche Testung oder aber



der Selbsttest positiv aus, darf zunächst nur für die Personalabteilung vermerkt werden, dass der betroffene Beschäftigte aufgrund eines positiven Selbsttests die Arbeitsstätte nicht betreten durfte. Darüberhinausgehende Meldepflichten, wie etwa eine an das zuständige Gesundheitsamt, können sich aus weiteren Regelungen ergeben.

In einigen Bundesländern dürfen Arbeitgeberinnen und Arbeitgeber nach erfolgtem negativem Selbsttest den getesteten Beschäftigten hierüber eine Bescheinigung ausstellen, die die getesteten Beschäftigten in dem Gültigkeitszeitraum für den Zutritt zu Einrichtungen nutzen können, die ebenfalls nur mit einer 3G-Bescheinigung betreten werden dürfen. Die Verarbeitung der Beschäftigtendaten für diese Bescheinigung kann nur mit einer freiwilligen und damit rechtswirksamen Einwilligung des betroffenen Beschäftigten erfolgen.

- **Sammeltransporte durch Arbeitgeberinnen und Arbeitgeber für Beschäftigte; § 28b Absatz 1 Satz 1 Variante 2, Absatz 3 IfSG**

Bieten Arbeitgeberinnen und Arbeitgeber Sammeltransporte für mehrere Beschäftigte zur Arbeitsstätte oder von der Arbeitsstätte an, so dürfen sie dies nur tun, wenn sie und ihre Beschäftigten zum Zeitpunkt des Transportes geimpft, genesen oder getestet sind und einen jeweiligen Nachweis darüber mit sich führen und zur Kontrolle bereithalten oder bei ihrer Arbeitgeberin oder ihrem Arbeitgeber hinterlegt haben.

Auch um Sammeltransporte durchführen zu können, dürfen Arbeitgeberinnen und Arbeitgeber daher jeweils die 3G-Daten ihrer Beschäftigten – soweit erforderlich – verarbeiten, § 28b Absatz 3 Satz 3 IfSG. Um Wiederholungen zu vermeiden, wird im Übrigen auf die obigen Ausführungen verwiesen.

- **Dokumentation der Nachweiskontrolle; § 28b Absatz 3 Satz 1 IfSG**

Nach dem Wortlaut der Vorschrift müssen Arbeitgeberinnen und Arbeitgeber die Einhaltung der Verpflichtungen der Beschäftigten, ihre Arbeitsstätten nur geimpft, genesen oder getestet zu betreten, durch Nachweiskontrollen täglich überwachen und regelmäßig dokumentieren, § 28b Absatz 3 Satz 1 IfSG. Der Vorschrift lässt sich nicht entnehmen, dass für diese Dokumentation personenbezogene Daten der kontrollierten Beschäftigten wie Vor- und Zunamen oder sogar eine differenzierte Dokumentation nach Impf-, Genesenen- oder Teststatus zu erfolgen hat. Deshalb muss an dieser Stelle geprüft werden, ob überhaupt und falls ja welche Beschäftigtendaten zur Erfüllung der Dokumentationspflicht erforderlich sind. Arbeitgeberinnen und Arbeitgeber werden für die Überprüfung der Zutrittsvoraussetzungen nachprüfbar Prozesse etablieren. Für die Erfüllung der Dokumentationspflicht wird es ausreichend sein, diesen Prozess, also durch wen und mit



welchen Mitteln erfolgt die Zutrittskontrolle, sowie das Datum der Zutrittskontrolle regelmäßig zu dokumentieren. Die personengenaue Speicherung von Gesundheitsdaten der Beschäftigten oder gar das Kopieren von 3G-Nachweisen der Beschäftigten wird in der Regel nicht erforderlich sein.

- **Anpassung eines betrieblichen Hygienekonzept; § 28b Absatz 3 Satz 4 IfSG**

Arbeitgeberinnen und Arbeitgeber dürfen die 3G-Daten ihrer Beschäftigten auch verarbeiten, soweit es für die Anpassung ihres betrieblichen Hygienekonzeptes auf Grundlage der Gefährdungsbeurteilung gemäß § 5 und § 6 ArbSchG erforderlich ist, § 28 Absatz 3 Satz 4 IfSG. Der Gesetzgeber hat damit eine ausdrückliche und zulässige Zweckänderung der Verarbeitung von 3G-Daten zugelassen. Ob personenbezogenen Daten der Beschäftigten für diesen Zweck erforderlich sind, muss im Einzelnen geprüft werden. Für die Anpassung des Hygienekonzeptes reichen gegebenenfalls anonymisierte oder pseudonymisierte Daten der Beschäftigten aus. Zudem ist die langfristige Speicherung von personengenauen (Klar-)Daten der Beschäftigten unzulässig.

- **Kontroll- und Servicepersonal in Verkehrsmitteln des Luftverkehrs, des öffentlichen Personennahverkehrs und des öffentlichen Personenfernverkehrs; § 28b Absatz 1 und Absatz 5 IfSG**

- Muss oder möchte das Kontroll- und Servicepersonal die Arbeitsstätten der genannten Beförderer betreten und ist an diesen ein Zusammentreffen mit anderen Personen nicht ausgeschlossen, so dürfen Beförderer deren 3G-Daten im Rahmen einer Zutrittskontrolle verarbeiten, § 28b Absatz 1 Satz 1, Absatz 3 Satz 3 IfSG. Um Wiederholungen zu vermeiden, wird an dieser Stelle nach oben verwiesen.
- Betritt nun das Kontroll- und Servicepersonal die Arbeitsstätte nicht, sondern nutzt lediglich die Verkehrsmittel der genannten Beförderer, dann ist Folgendes zu beachten: Neben den Flug- und Fahrgästen muss auch das Kontroll- und Servicepersonal geimpft, genesen oder getestet sein, um die Beförderungsmittel nutzen zu dürfen, § 28 b Absatz 5 Satz 1 IfSG. Die Beförderer sind verpflichtet, unter anderem die Einhaltung dieser Verpflichtung durch stichprobenhafte Nachweiskontrollen zu überwachen. Alle beförderten Personen sind verpflichtet, auf Verlangen einen Impf-, Genesenen- oder Testnachweis vorzulegen. Beförderer können zu diesem Zweck die 3G-Daten unter anderem ihres Kontroll- und Servicepersonals verarbeiten. Damit dürfen Beförderer mindestens Einsicht in die 3G-Daten ihres Kontroll- und Servicepersonals nehmen. Mit Einwilligung der jeweiligen Person

wäre auch die Speicherung des Impf- sowie Genesenenstatus (2G-Daten) möglich. Dann müssten die Beförderer die 2G-Daten ihrer entsprechenden Beschäftigten nicht erneut abfragen.

- **Verarbeitung auf Grundlage von Rechtsverordnungen**

Arbeitgeberinnen und Arbeitgeber dürfen die 3G-Daten von Beschäftigten auch verarbeiten, soweit dies durch Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG vorgegeben ist.

- **Verarbeitung im Gesundheitsbereich; § 23a, § 23 Absatz 3 IfSG**

Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber aus dem Gesundheitsbereich (Krankenhäuser, Arztpraxen usw.) dürfen unter den in § 23a, § 23 Absatz 3 IfSG genannten gesetzlichen Voraussetzungen den Impf- und Serostatus ihrer Beschäftigten verarbeiten.

- **Verarbeitung in besonderen Einrichtungen; § 36 Absatz 3 IfSG**

Bestimmte – im Gesetz genannte – Arbeitgeberinnen und Arbeitgeber, zum Beispiel Trägerinnen und Träger von Kindertageseinrichtungen, ambulante Pflegedienste usw., dürfen unter den in § 36 Absatz 3 IfSG genannten Voraussetzungen den Impf- und Serostatus ihrer Beschäftigten im Zusammenhang mit COVID-19 verarbeiten.

- **Verarbeitung zum Zweck der Entschädigung; § 56 Absatz 1 IfSG**

Arbeitgeberinnen und Arbeitgeber dürfen den Impfstatus derjenigen Beschäftigten verarbeiten, die ihnen gegenüber einen Anspruch auf Geldentschädigung (Lohnersatz) nach § 56 Absatz 1 IfSG geltend machen. Dessen Voraussetzungen können im Einzelfall auch im Fall einer möglichen Infektion mit COVID-19 (insbesondere wenn die/der Beschäftigte Kontaktperson ist) sowie einer sich anschließenden Quarantäne vorliegen. Anspruchsvoraussetzung ist unter anderem, ob die Möglichkeit einer Schutzimpfung gegen das Coronavirus SARS-CoV-2 bestand. Die/der Beschäftigte ist allerdings nicht verpflichtet, der Arbeitgeberin oder dem Arbeitgeber seinen Impfstatus offen zu legen. Die/der Beschäftigte kann die Entschädigung auch selbst bei der jeweils für ihn zuständigen Behörde verlangen, § 56 Absatz 5 Satz 4 IfSG.

Im Zusammenhang mit der Verarbeitung der Gesundheitsdaten von Beschäftigten sind weiter zu beachten:

- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Zunächst muss geprüft werden, ob die reine Abfrage der Gesundheitsdaten zur Zweckerreichung bereits ausreichend ist. Dann ist keine Speicherung erforderlich. Sollen die Gesundheitsdaten gespeichert werden, dürfen keine Nachweise (im Original oder in Kopie) in die Personalakte aufgenommen werden. Es ist ausreichend, wenn im Fall des § 28b IfSG auf Listen vermerkt wird, dass diese jeweils vorgelegt worden sind.
- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e DS-GVO, Recht auf Löschung, Artikel 17 DS-GVO:  
Sobald der Zweck für die Speicherung der Gesundheitsdaten entfallen ist, müssen die personenbezogenen Daten gelöscht werden. Das Gesetz sieht derzeit für 3G-Daten eine maximale Speicherdauer von sechs Monaten vor, § 28b Absatz 3 Satz 9 IfSG. Eine Löschung kann indes auch früher erforderlich sein, wenn der jeweilige Zweck entfallen ist; zum Beispiel, wenn die Gültigkeitsdauer des jeweiligen Nachweises – so bei einem Antigen-Schnelltest nach 24 Stunden – abgelaufen ist, wird eine darüberhinausgehende Speicherung diesbezüglicher personenbezogener Daten zum Zwecke der Zutrittskontrolle regelmäßig nicht mehr erforderlich sein. Darüber hinaus ist die nach § 28b Absatz 7 IfSG begrenzte Geltungsdauer der gesetzlichen Rechtsgrundlagen zu berücksichtigen.
- Grundsatz der „Integrität und Vertraulichkeit“, Artikel 5 Absatz 1 Buchstabe f DS-GVO, § 22 Absatz 2 Nummer 5; Nummer 8 BDSG:  
Arbeitgeberinnen und Arbeitgeber müssen für die Zutritts- beziehungsweise Nachweiskontrollen geeignete Beschäftigte oder Dritte einsetzen. Dritte sind zur Verschwiegenheit zu verpflichten, Beschäftigte sind auf ihre – auch innerbetrieblich geltende – Verschwiegenheitspflicht zu sensibilisieren. Der Kreis der Personen, die Zugang zu den 3G-Daten haben und verarbeiten, ist so klein wie möglich zu halten. Setzen Arbeitgeberinnen und Arbeitgeber Dritte ein, muss mit diesen gegebenenfalls ein Auftragsverarbeitungsvertrag geschlossen werden (Artikel 28 DS-GVO). Werden die Gesundheitsdaten auch für die Anpassung eines betrieblichen Hygienekonzeptes verarbeitet, so dürfen diese Daten – soweit erforderlich – auch den mit dessen Anpassung beauftragten Beschäftigten zur Verfügung gestellt werden. Erforderlich wäre dies zum Beispiel dann nicht, wenn es bei den Hygienemaßnahmen nicht darauf ankommt, welcher Beschäftigter im Einzelnen geimpft, genesen oder aber getestet ist. Im Regelfall dürften – wie ausgeführt – für die Anpassung des Hygienekonzeptes anonymisierte oder pseudonymisierte Beschäftigtendaten genügen.
- Grundsatz der „Rechenschaftspflicht“, Artikel 5 Absatz 2 DS-GVO:  
Arbeitgeberinnen und Arbeitgeber müssen – sofern einschlägig – auch die Freiwilligkeit einer Einwilligung nachweisen können, Artikel 7 Absatz 1 DS-

GVO. Aufgrund des zwischen Arbeitgeberinnen und Arbeitgebern sowie ihren Beschäftigten bestehenden Über- und Unterordnungsverhältnisses bestehen regelmäßig Zweifel an der Freiwilligkeit und damit Rechtswirksamkeit der Einwilligung von Beschäftigten. Im Beschäftigtendatenschutz kann Freiwilligkeit insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (§ 26 Absatz 2 Satz 2 BDSG). Bei der Pandemiebekämpfung können gleichgelagerte Interessen vorliegen.

- Für die Verarbeitung der 3G-Daten nach § 28b Absatz 3 IfSG gilt zudem § 22 Absatz 2 BDSG entsprechend.  
§ 22 Absatz 2 BDSG verpflichtet die Verantwortliche – hier die Arbeitgeberinnen und Arbeitgeber – dazu, angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen vorzusehen. Zu den Maßnahmen kann zum Beispiel insbesondere die Verschlüsselung digitalen Listen mit den 3G-Daten gehören, § 22 Absatz 2 Nummer 7 BDSG. Wo immer möglich sollte eine anonymisierte und, wenn Anonymisierung nicht möglich ist, eine pseudonymisierte Verarbeitung erfolgen (§ 22 Absatz 2 Nummer 6 BDSG). Auch sollten die technischen und organisatorischen Maßnahmen so gestaltet werden, dass angemessen berücksichtigt wird, dass es sich um eine besondere Kategorie personenbezogener Daten im Sinne des Artikel 9 DSGVO handelt. Wegen der weiteren Einzelheiten wird auf § 22 Absatz 2 BDSG verwiesen.

## **9. Dürfen Arbeitgeberinnen und Arbeitgeber für ihre Beschäftigten Impftermine organisieren und in diesem Zusammenhang pbD verarbeiten?**

### **Antwort:**

Ja, mit wirksamer Einwilligung ihrer Beschäftigten.

Organisieren Arbeitgeberinnen und Arbeitgeber zentral die Impfung ihrer Beschäftigten, dürfen sie die Beschäftigtendaten an das Impfzentrum nur mit deren jeweiligen Einwilligungen übermitteln. Zu den einzelnen Voraussetzungen einer freiwillig und damit rechtswirksam erteilten Einwilligung der Beschäftigten siehe Frage 1.

In diesem Zusammenhang sind weiter zu beachten:

- Grundsatz der „Datenminimierung“, Artikel 5 Absatz 1 Buchstabe c DS-GVO: Möglicherweise reicht an dieser Stelle durch Arbeitgeberinnen und Arbeitgeber nur die Übermittlung der Namen der Beschäftigten aus. Gesundheits-

daten, die Beschäftigte im Zusammenhang mit einer Impfung an die Impfen- den offenlegen müssen, sollten nur gegenüber den Impfen- den offenge- legt werden: Zum Beispiel indem sie Formulare, mit denen Gesundheitsda- ten abgefragt werden, den Impfen- den (Betriebsarzt, Impfzentrum) selbst übermitteln.

Vermerke in der Personalakte der betroffenen Beschäftigten über die An- meldung zur Impfung sind unzulässig.

- Grundsatz der „Speicherbegrenzung“, Artikel 5 Absatz 1 Buchstabe e, Recht auf Löschung, Artikel 17 DS-GVO:

Nach einer erfolgten Anmeldung und einer sich hieran gegebenenfalls an- schließenden Abrechnung der Impfung, zum Beispiel durch externe Be- triebsärzte, sind die pbD der betroffenen Beschäftigten aufgrund der Zwe- ckerfüllung zu löschen.

- Da bereits die Impfwillingkeit ein Gesundheitsdatum ist, Artikel 4 Nummer 15 DS-GVO, muss sich die Einwilligung der Beschäftigten ausdrücklich auf dieses Datum beziehen, § 26 Absatz 3 Satz 2 BDSG.