DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

Datenschutz bei Maßnahmen gegen die Ausbreitung des Corona-Virus in Unternehmen

(Stand: 24.03.2020)

Das Datenschutzrecht ist gerade auch bei der Umsetzung von Maßnahmen zur Verhinderung der Ausbreitung des Corona-Virus (Covid-19) zu beachten! Es gibt – derzeit und absehbar - keine pauschalen Befreiungen oder auch nur Erleichterungen. Das zwingt Sie aber nicht in den Konflikt, das eine zu lassen oder gegen das andere verstoßen zu müssen. Mit einem strukturierten Ansatz bekommen Sie beides „unter einen Hut“.

1. Stufenkonzept

Die pauschale Musterlösung gibt es nicht. Dazu sind die Konstellationen zu verschieden und verändern sich zu schnell. Daher gibt es leider kein „one size fits all“. Hinzu kommt, dass die Entwicklung derzeit so rasant ist, dass vorgestern noch als unzulässig betrachtete Maßnahmen heute zulässig sein können. Aber dennoch gilt nicht, dass der Zweck die Mittel heiligt.

Wir wollen Ihnen daher eine pragmatische, aber dafür nicht ins datenschutzrechtliche Detail ausdifferenzierte Herangehensweise vorstellen. Damit können Sie Ihre Maßnahme(n) einordnen und schnell bewerten. Der Rechtsrat kann hierdurch nicht ersetzt, aber vereinfacht werden. Wenden Sie sich an uns, wenn Sie Unterstützung benötigen!

Nicht jede Maßnahme erfordert die Verarbeitung personenbezogener Daten und manche Maßnahme ist als Vorstufe der Verarbeitung personenbezogener Daten erforderlich. Mit folgendem Stufenkonzept können Sie an die Bewertung der Maßnahmen rangehen:

Stufenkonzept mit zunehmenden rechtlichen Anforderungen			
1.	Maßnahmen ohne Verarbeitung personen-bezogener Daten	<u>Beispiele:</u> Verhaltensregeln, Hygienehinweise, Verhaltensregeln für Lieferanten (bis hin zum Verlassen der Fahrer-kabine), Untersagung des Zugangs bei nicht zwingenden Zutritten	Keine Datenschutz-pflichten zu beachten! <u>Achtung:</u> Dies ändert sich, wenn die Einhaltung der Maßnahmen überprüft wird und erfasst wird.
2.	Verarbeitung normaler personenbezogener Daten <u>Hinweis:</u> Für Beschäftigte und Externe gelten verschiedene Rechtsgrundlagen	<u>Beispiele:</u> Herkunft aus „Sperrgebieten“ oder „Risikogebieten“ oder Kontakten zu Infizierten (ohne Nachfrage, wer der Infizierte ist und ob Familienangehöriger usw.), aber auch Einsatz- und Arbeitspläne.	Als Rechtsgrundlagen kommen § 26 Abs. 1 S. 1 BDSG für Beschäftigte und Art. 6 Abs. 1 Satz 1 lit f. DS-GVO für alle anderen Personen in Betracht. <u>Voraussetzung:</u> Abwägung der Interessen
3.	Verarbeitung von Gesundheitsdaten <u>Hinweis:</u> Für Beschäftigte und Externe gelten verschiedene Rechtsgrundlagen „*Gesundheitsdaten*“ sind *„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheits-dienstleistungen, beziehen und aus denen*	<u>Beispiele:</u> Fiebermessungen beim Zutritt, Homeoffice-Planungen unter Berücksichtigung von Zuordnungen zu gesundheitlichen Gefährdungsgruppen. <u>Beispiel:</u> Abfrage von Selbsteinordnung in Risikogruppen zur Gestaltung von Homeoffice-Plänen.	Als Rechtsgrundlage kommt § 26 Abs. 3 BDSG für Beschäftigte in Betracht. <u>Voraussetzung:</u> Abwägung der Interessen. Für alle anderen Personen ist die Wahl der rechtlichen Begründung derzeit nicht ohne Weiteres möglich.

	Informationen über deren Gesundheitszustand hervorgehen“ (Art. 4 Nr. 15 DS-GVO).		
4.	Maßgaben für alle Verarbeitungen, insbesondere:		
	4.1 Datenminimierung	Verarbeiten Sie nur die Daten, die begründbar erforderlich sind.	Beispiel: Sie müssen nicht immer wissen, mit welcher infizierten Person Kontakt bestand. Denn allein der Umstand genügt.
	4.2 Begrenzung des Zugriffs	Nicht jeder Mitarbeiter muss diese Daten einsehen können.	Beispiel: Nicht jeder Mitarbeiter muss in einem Einsatzplan lesen können, welche Kollegen zu einer Risikogruppe gehören.
	4.3 Festlegung der Speicher-dauer	Die Daten müssen nicht unendlich gespeichert bleiben.	Die Verarbeitung muss am Zweck ausgerichtet sein.
	4.4 Festlegung der Sicherheit der Verarbeitung	Die Daten müssen technisch-organisatorisch geschützt sein.	
	4.5 Unterrichtung jeder betroffenen Person bei der jeweiligen Datenerhebung nach Maßgabe der Artt. 12, 13, 14 DS-GVO.	Vereinfacht zum Zusammenstellen der Inhalte: Jeder muss informiert werden, wer was mit welchen Daten wozu (zu welchem/n Zwecke/n) warum (berechtigtes Interesse) wie lange!	Achtung: Der Umfang der Pflichtinhalte nach Artt. 13, 14 DS-GVO geht natürlich weiter, aber mit der links stehenden Faustformel ist die Vorbereitung leichter! **Achtung:** Erheben Sie Daten nicht direkt bei der jeweiligen Person, sondern mittelbar (bspw. Angehörige Person eines Mitarbeiters) dann müssen Sie

			grundsätzlich auch diese Person benachrichtigen!
	Achtung: Wenn Sie personenbezogene Daten nicht direkt bei der jeweiligen Person, sondern mittelbar erheben (bspw. Nachfrage bei Mitarbeiter zur Gesundheit von Angehörigen), dann müssen Sie grundsätzlich auch diese Person benachrichtigen (Art. 14 DS-GVO)! Es gibt Ausnahmen, aber die müssen geprüft und dokumentiert werden. Machen Sie es sich einfacher, wenn es schnell gehen muss und verzichten Sie auf solche Informationen, wenn es vermeidbar ist.		
Exkurs:	Einwilligung der betroffenen Person	Formal betrachtet kommt auch die Einwilligung der betroffenen Person in Betracht. Diese muss jedoch freiwillig erteilt werden. Hieran bestehen Zweifel, wenn keine echte Wahlmöglichkeit besteht. Gerade im Beschäftigungsverhältnis wird dies nicht leicht zu begründen sein.	
<u>Tipp:</u> Die Verarbeitung muss im Rahmen einer Interessenabwägung gerechtfertigt werden (können). Auch für diese ist die Beschreibung anhand des vorstehenden Stufenkonzepts wichtig, um deutlich zu machen, dass für die betroffene Person mildere Mittel (auch) erfolgt sind oder zumindest in Betracht gezogen wurden.			

2. Besonders heikel: Offenlegung der Identität von infizierten Beschäftigten oder entsprechendem Verdacht gegenüber anderen Beschäftigten

Besonders problematisch ist die Offenlegung der Identität von infizierten Beschäftigten oder einem entsprechenden Verdacht gegenüber anderen Beschäftigten und Dritten.

Der Grundsatz muss sein: Nur, wenn es zwingend ist und nur an diejenigen, die zwingend Kenntnis haben müssen. Der Name nur, wenn es für diese Maßnahme zwingend erforderlich ist.

Das bisher zur Verneinung herangezogene Argument der Stigmatisierung halte ich – entgegen der FAQ der Datenschutzaufsichtsbehörde Baden-Württemberg (siehe Link unten) – zwar zwischenzeitlich nicht mehr für so durchschlagend, aber wer hierzu Recht behält, ist noch nicht geklärt. Ich sehe aber ein großes Risiko in einer zu laxen Kommunikation bei Einsatz- und Arbeitsplänen (auch bzgl. Homeoffice), wenn darin für jeden erkennbar ist, welcher Kollege ein Risikopatient ist (oder gar noch warum das so ist). Aber Risiken bestehen bei der Offenlegung weiterhin – vielleicht weniger mit Blick auf ein Bußgeld als eher mit Blick auf Schadensersatzansprüche in „raueren Zeiten“.

Die Aufsichtsbehörde Baden-Württemberg schlägt ein dreistufiges Vorgehen vor (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/FAQ-Corona.pdf):

1. Schutzmaßnahmen und Warnung ohne Offenlegung.
2. Ist dies ausnahmsweise nicht ausreichend, so muss der Arbeitgeber Kontakt mit den Gesundheitsbehörden aufnehmen und um deren Entscheidung ersuchen.
3. Ist auch dies nicht möglich, dürfen auch die übrigen Mitarbeiter über den Verdacht der Ansteckung oder der Erkrankung des konkreten Mitarbeiters informiert werden, um Infektionsquellen zu lokalisieren und einzudämmen.

3. Home-Office-Regelungen

Die Arbeit im Home-Office bringt ebenfalls Datenschutzfragen mit sich und zwar in zwei Richtungen:

1. Verarbeitung der Daten des Beschäftigten und
2. Verarbeitung von personenbezogenen Daten durch den Beschäftigten im Rahmen seiner Tätigkeit für den Arbeitgeber.

Wenn das Unternehmen noch keine Regelungen hat, aber die Zeit sehr drängt, bietet sich eine Orientierung an den Vereinbarungen über die Auftragsverarbeitung nach Art. 28 DS-GVO an. Natürlich passen die nicht eins-zu-eins. Sie können aber als Orientierung und Checkliste für Inhalte verwendet und schnell angepasst werden. Denn die wichtigsten Punkte für eine Home-Office-Regelung sind ebenfalls: Weisungsgebundenheit bei der Verarbeitung (Art. 29 DS-GVO), technisch-organisatorischer Schutz der Daten im Home-Office (Art. 32 DS-GVO – Stichworte: Kein Zugriff durch Dritte, Datensicherung, keine unnötigen Ausdrucke und deren Vernichtung im Büro, akustischer Schutz bei Telefonaten & Co., technischer Schutz der Endgeräte sowie der Zugangssysteme, Geheimhaltung von Zugangs-/Zugriffsberechtigungen) und Meldung bei Datenschutzpannen sowie Festlegung des Standorts anhand Wohnanschrift.

Die Datenerhebung und -speicherung in Bezug auf die Arbeit/Tätigkeit des Beschäftigten (Log-In, Log-Out, Firewalls, Last der Systeme, Bearbeitungsstand von Unterlagen und Ablagen) lässt sich durch § 26 Abs. 1 S. 1 BDSG rechtfertigen, sofern dies angemessen ausgestaltet ist. Diese Erfassung kann auch mitbestimmungspflichtig sein. Entscheidend ist die Beachtung der proaktiven Informationspflichten nach Artt. 12, 13, 14 DS-GVO.

Gerne erstellen wir für Sie entsprechende Mustervereinbarungen und Hinweise!

4. Bußgelder und Schadensersatzansprüche

Weder die Bußgeld- noch die Schadensersatzregelungen der DS-GVO sind durch die „Corona-Bekämpfung“ außer Kraft gesetzt. Auch hier gilt: Der Zweck heiligt nicht die Mittel! Allerdings setzen sowohl Geldbußen als auch Schadensersatzansprüche nach deutschem Rechtsverständnis ein Verschulden voraus. Das ist allerdings – vor allem EU-weit – nicht unumstritten.

Unser Ratschlag daher: Handeln sie klar, aber besonnen. Dokumentieren Sie, warum Sie was wie für erforderlich gehalten haben. Machen Sie deutlich, dass Sie nicht unbedacht und nicht nach dem Motto „Der Zweck heiligt die Mittel“ verfahren sind.

Bitte beachten Sie aber vor allem die flankierenden Regelungen des Datenschutzrechts – allen voran die Informationspflichten, Löschfristen, Zugriffsberechtigten und Vermeidung unnötiger Offenbarung von Gesundheitszuständen. Denn diese eignen sich besonders gut für Schadensersatz- und Schmerzensgeldansprüche.

Und lassen Sie uns nüchtern sein, wenn die wirtschaftliche Lage infolge der Krisen angespannter ist, ist auch die Bereitschaft zur Geltendmachung von Schadens- und Schmerzensgeldforderungen größer. Hier kann ein „Bumerang“ drohen!

Kurzum: Ignorieren Sie nicht die datenschutzrechtlichen Vorgaben. Es geht dabei nicht nur um die Frage, zulässig oder unzulässig. Auch eine zulässige Maßnahme kann zu einem Verstoß bei Missachtung „flankierender“ Pflichten führen. Wir unterstützen Sie bei der Gestaltung und bei der Abwehr von Ansprüchen!

5. Hinweise der Aufsichtsbehörden

Die Aufsichtsbehörden in der EU haben keine einheitliche Linie. Während einige zu pragmatischer Lockerung tendieren, mahnen andere die Strenge. Nachfolgend einige Hinweise auf Veröffentlichungen der deutschen Datenschutzaufsichtsbehörden (**Stand: 23.03.2020**):

- LfDI Baden-Württemberg: „Häufig gestellte Fragen („FAQs“) zum Thema Corona“: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/FAQ-Corona.pdf (Stand: 23.03.2020)
- Der BfDI gibt folgenden Hinweis (https://www.bfdi.bund.de/DE/Datenschutz/-Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154 (Stand: 23.03.2020)) – die rechtliche Begründung finden Sie ebenfalls unter diesem Link:

„Beispielsweise können die folgenden Maßnahmen zur Eindämmung und Bekämpfung der Corona-Pandemie als datenschutzrechtlich legitimiert betrachtet werden:

- *Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Beschäftigten durch den Arbeitgeber oder Dienstherren um eine Ausbreitung des Virus unter den Beschäftigten bestmöglich zu verhindern oder einzudämmen. Hierzu zählen insbesondere Informationen zu den Fällen:*
- *in denen eine Infektion festgestellt wurde oder Kontakt mit einer nachweislich infizierten Person bestanden hat.*
- *in denen im relevanten Zeitraum ein Aufenthalt in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet stattgefunden hat.*
- *Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern, insbesondere um festzustellen, ob diese selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen.*
- *sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben.*
- *Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist demgegenüber nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist.“*

- Hinweise des BayLDA zu Datenschutz und Datensicherheit: https://www.lda.bayern.de/de/corona_datenschutz.html (Stand: 23.03.2020)
- LDA Brandenburg: „Corona-Pandemie: Datenschutz und Heimarbeit“: https://www.lda.brandenburg.de/media_fast/4055/Heimarbeit_200323.pdf (Stand: 23.03.2020)
- Die LfDI Bremen gibt auf der ersten Seite der Pressemitteilung vom 20.03.2020 Hinweise zur Verarbeitung von Gesundheitsdaten im Beschäftigungsverhältnis: „Die Landesbeauftragte für Datenschutz legt ihren zweiten Tätigkeitsbericht nach der DSGVO vor: Der Tanker nimmt Fahrt auf“ https://www.datenschutz.bremen.de/ (Stand: 23.03.2020)
- Hinweise des LfDI Rheinland-Pfalz zum Thema „Corona und Beschäftigtendatenschutz“: https://www.datenschutz.rlp.de/de/themenfelder-themen/beschaeftigtendatenschutz-corona/ (Stand: 23.03.2020)
- Die Datenschutzaufsichtsbehörden der Bundesländer Berlin, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Sachsen-Anhalt und Schleswig-Holstein verweisen jeweils auf die Stellungnahme des BfDI (siehe oben). Die Datenschutzaufsichtsbehörde Nordrhein-Westfalen verweist zusätzlich auf die FAQs des LfDI Baden-Württemberg (siehe oben). Auf den Internetseiten der Datenschutzaufsichtsbehörden von Sachsen und Thüringen konnten wir zum Zeitpunkt der Fertigstellung dieses Beitrags keine speziellen Angaben zum Thema finden.

Ihr Ansprechpartner:
Rechtsanwalt Dr. Jens Eckhardt, Fachanwalt für Informationstechnologierecht
Derra, Meyer & Partner Rechtsanwälte PartGmbB, Düsseldorf, Ulm, Berlin
Datenschutz-Auditor (TÜV), Compliance Officer (TÜV), Mitglied im Vorstand des Berufsverbands der Datenschutzbeauftragten (BvD) e.V.
Immermannstraße 15, 40210 Düsseldorf -Tel: +49(0)211/17520660 - Fax: +49(0)211/17520666
E-Mail: eckhardt@derra-d.de - www.derra.eu