SAXINGER
law. tax. clarity.

COVID-19 und DSGVO

- Welche Daten des Mitarbeiters darf der Arbeitgeber verarbeiten und welche Daten gelten dabei als besonders geschützte Gesundheitsdaten?
- Doch inwieweit ist das zulässig? Oder ist das sogar verpflichtend?
- Dürfen oder müssen diese Daten an Behörden oder Konzerngesellschaften weitergeleitet werden?
- Wer darf diese Daten im Unternehmen einsehen?
- Muss diese Datenverarbeitung unternehmensintern besonders dokumentiert werden?
- Wie lange darf man die Daten speichern?
- Wie setzt man die gesetzlichen Datensicherheitsmaßnahmen bei Home-Office um?
- Muss für sämtliche Verarbeitungen eine Einwilligung eingeholt werden?
- Welche Rechte können Mitarbeiter gegenüber dem Arbeitgeber hinsichtlich der Verarbeitung ihrer Daten ausüben?
- Für welche Verarbeitungen muss eine Datenschutzfolgenabschätzung (DSFA) durchgeführt werden?

Welche Daten des Mitarbeiters darf der Arbeitgeber verarbeiten und welche Daten gelten dabei als besonders geschützte Gesundheitsdaten?

Im Rahmen des Arbeitsverhältnisses verarbeitet der Arbeitgeber eine Reihe von personenbezogenen Daten seiner Mitarbeiter. Diese personenbezogenen Daten können etwa einfache Stamm- und Adressdaten (Name, Adresse, E-Mail, Telefonnummer), Daten zum konkreten Arbeitsverhältnis (Position, Gehaltsstufe, Sozialversicherungsnummer), aber auch Gesundheitsdaten sein (zB Anzahl der Krankenstandstage).

Gesundheitsdaten werden in der Datenschutzgrundverordnung (DSGVO) als besondere Datenkategorie einem **strengeren Schutz** unterworfen. Im Zusammenhang mit COVID-19 können **folgende Angaben Gesundheitsdaten** darstellen:

- Angaben, ob eine Person mit dem Virus infiziert ist;
- Angabe, ob eine Person mit einer infizierten Person Kontakt hatte und demnach der Verdacht einer Erkrankung besteht;
- Angabe, ob sich eine Person in einem Risikogebiet aufgehalten hat;
- Einschätzung, ob eine Person zu einer Risikogruppe zählt;
- Physiologische (Sensor-)Daten, zB die Körpertemperatur oder (Selbst-)Auskünfte zum Gesundheitszustand.

Bei der Verarbeitung dieser Daten sind die **Grundsätze der Datenverarbeitung zwingend einzuhalten**. So muss etwa geprüft werden, ob die Verarbeitung zur Erreichung eines konkreten Zwecks erforderlich ist und ob nur diejenigen Daten verarbeitet werden, die zur Zweckerreichung erforderlich sind.

Doch inwieweit ist das zulässig? Oder ist das sogar verpflichtend?

Für die Verarbeitung können folgende Rechtsgrundlagen bestehen:

- **Einwilligung der betroffenen Person,** wobei die erforderliche Freiwilligkeit im Hinblick auf das Verhältnis zwischen Arbeitgeber und Arbeitnehmer genau zu hinterfragen ist;
- **Verpflichtung des Arbeitgebers,** die ihm bzw. dem Arbeitnehmer zukommenden Rechte aus dem **Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes wahrnehmen zu können.** Dies betrifft insbesondere Fälle, in denen der Arbeitgeber aufgrund der ihm arbeitsvertraglich zukommenden Fürsorgepflicht die Sicherheit seiner Arbeitnehmer gewährleisten muss;
- Der Arbeitgeber ist zur Verarbeitung aus Gründen des **öffentlichen Interesses** im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren berechtigt oder verpflichtet. Eine entsprechende Berechtigung im Katastrophenfall enthält § 10 Abs 2 DSG, eine Verpflichtung zur Meldung besteht etwa nach dem Epidemiegesetz 1950.
- Der Arbeitgeber ist aus Gründen der **Gesundheitsvorsorge oder der Arbeitsmedizin**, etwa aufgrund einer

Betriebsvereinbarung, zur Verarbeitung berechtigt.

Dürfen oder müssen diese Daten an Behörden oder Konzerngesellschaften weitergeleitet werden?

Nach § 5 Abs 3 Epidemiegesetz 1950 sind (ua) **Arbeitgeber auf Verlangen der Bezirksverwaltungsbehörde zur Auskunftserteilung verpflichtet**. Diese Auskunft erstreckt sich auch auf alle Verdachtsfälle meldepflichtiger Krankheiten, wozu nach § 1 Abs 1 Z 1 Epidemiegesetz 1950 auch das „*neue Corona-Virus*" zählt.

Eine **Weiterleitung an Konzernunternehmen** ist am genauen **Zweck der Datenübermittlung** zu messen. Auch hier sind wiederum die Grundsätze der Datenverarbeitung zu beachten und zu eruieren, ob mit anonymisierten Daten das Auslangen gefunden werden kann.

Wer darf diese Daten im Unternehmen einsehen?

Die Anzahl der einsichtsberechtigten Personen sollte auf ein Minimum beschränkt werden. Ein Zugriff auf die Daten erfolgt dabei in aller Regel durch die **HR-Abteilung, die Geschäftsführung sowie einen allfällig vorhandenen Betriebsarzt.** Aufgrund der Diskriminierungsgefahr ist von der Information sämtlicher Arbeitnehmer in einem Betrieb, dass ein konkret benannter Mitarbeiter erkrankt sei, abzusehen. Vielmehr sollte eine allgemeine, anonymisierte Information erfolgen, dass es einen Krankheitsfall gegeben hat.

Muss diese Datenverarbeitung unternehmensintern besonders dokumentiert werden?

Die mit COVID-19 in Verbindung stehenden Verarbeitungen sind im **Verarbeitungsverzeichnis nach Art 30 Abs 1 DSGVO** entsprechend abzubilden. Im Hinblick auf die Verarbeitung von Gesundheitsdaten sollte besonders dokumentiert werden, wie die Grundsätze der Datenverarbeitung eingehalten werden, zumal der Arbeitgeber für deren Einhaltung rechenschaftspflichtig ist.

Wie lange darf man die Daten speichern?

Dem allgemeinen Grundsatz der Speicherbegrenzung folgend müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung des Arbeitnehmers nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Liegt der Zweck daher etwa in der Wahrnehmung der **Fürsorgepflicht des Arbeitgebers,** dürfen Daten eines erkrankten Arbeitnehmers **bis zum Zeitpunkt seiner Gesundung** gespeichert werden. Daten zu Arbeitnehmern, die als Verdachtsfälle gespeichert wurden, sind zu löschen, sobald sich der Verdacht einer Erkrankung nicht bewahrheitet.

Wie setzt man die gesetzlichen Datensicherheitsmaßnahmen bei Home-Office um?

Der Einsatz privater Devices (Bring your own device – BYOD) ist vor dem Hintergrund, dass der Arbeitgeber als datenschutzrechtlich Verantwortlicher Maßnahmen zum Schutz von personenbezogenen Daten etwa von Kunden und Arbeitnehmern zu setzen hat, kritisch zu sehen. So ist es etwa möglich, dass vertrauliche Daten von Kunden und Arbeitnehmern über Synchronisationslösungen (Dropbox, OneDrive, Google Drive), die privat vom Arbeitnehmer installiert wurden, in einer Cloud gespeichert werden. Darüber hinaus bestehen auch Risiken im Bereich der Cybersicherheit.

Sofern ausreichende Ressourcen bestehen, sollten Arbeitnehmern für das Home-Office **Firmen-Laptops** zur Verfügung gestellt bekommen, die mittels sicherer **Virtual Private Network (VPN)-Verbindung in das Firmennetz eingebunden** werden. Wenn dennoch **Privat-Laptops** (etwa mangels Ressourcen) zum Einsatz kommen, sollte auf **Remote-Desktop-Lösungen** zurückgegriffen werden, die mittels sicherer Protokolle eine Verbindung auf den Desktop des Arbeitsgeräts am Firmenstandort herstellen.

Muss für sämtliche Verarbeitungen eine Einwilligung eingeholt werden?

Nein. Es bestehen unterschiedliche Rechtsgrundlagen, nach welchen eine Verarbeitung zulässig ist, ohne dass von der betroffenen Person eine Einwilligung eingeholt werden muss. So bestehen für öffentliche Stellen bzw. Behörden besondere

Rechtsgrundlagen, die auf einer gesetzlichen Ermächtigung oder Verpflichtung zur Verarbeitung gründen.

Auch für Arbeitgeber besteht eine Reihe unterschiedlicher Rechtsgrundlagen. *(*Siehe Frage: *Doch inwieweit ist das zulässig? Oder ist das sogar verpflichtend?)*

Welche Rechte können Mitarbeiter gegenüber dem Arbeitgeber hinsichtlich der Verarbeitung ihrer Daten ausüben?

Arbeitgeber sind als datenschutzrechtlich Verantwortliche zur Wahrnehmung der Rechte ihrer Arbeitnehmer nach den Art 15 – 22 DSGVO verpflichtet. So haben **Arbeitnehmer insbesondere folgende Rechte:**

- **Recht auf Auskunft nach Art 15 DSGVO.** Anzugeben sind dabei insbesondere die Zwecke der Verarbeitung, die Kategorien der verarbeiteten personenbezogenen Daten, die Empfänger bzw. Kategorien der Empfänger sowie die Speicherdauer;
- **Recht auf Berichtigung nach Art 16 DSGVO.** Arbeitnehmer können daher vom Arbeitgeber verlangen, über sie gespeicherte personenbezogene Daten zu berichtigen, oder – in bestimmten Fällen – zu ergänzen;
- **Recht auf Löschung nach Art 17 DSGVO** unter bestimmten Voraussetzungen. Dieses Recht besteht insbesondere dann nicht, wenn der Arbeitgeber aufgrund einer rechtlichen Verpflichtung zur Verarbeitung der Daten verpflichtet ist;
- **Recht auf Einschränkung der Verarbeitung nach Art 18 DSGVO** unter bestimmten Voraussetzungen.

Für welche Verarbeitungen muss eine Datenschutzfolgenabschätzung (DSFA) durchgeführt werden?

Die Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung hängt von mehreren Faktoren ab, wobei insbesondere die Verwendung neuer Technologien, die Art, Umfang, Umstände und Zwecke der Verarbeitung zu berücksichtigen sind. Eine **DSFA** ist durchzuführen, wenn bei Berücksichtigung aller Umstände eine **Verarbeitung voraussichtlich zu einem hohen Risiko für betroffene Personen** führt.

Denkbar ist die Durchführung einer DSFA etwa, wenn mittels künstlicher Intelligenz versucht wird, durch umfangreiches Datenmaterial Rückschlüsse auf den Gesundheitszustand betroffener Personen zu ziehen und daraus bestimmte Konsequenzen abzuleiten, etwa, ob die Person erkrankt ist. Die Datenschutzbehörde hat in ihrer *Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist*, eine Liste veröffentlicht, bei welchen Verarbeitungen eine DSFA durchzuführen ist.

Unsere Experten der **SAXINGER COVID-19-Unit** stehen Ihnen in diesem Zusammenhang gerne beratend zur Seite.

Dr. Philipp L. Leitner
Rechtsanwalt
Linz
T +43 732 603030-539
F +43 732 603030-500
p.leitner@saxinger.com