Digitalisierung und datenschutzrechtliche Fragen im Zusammenhang mit COVID-19

Verarbeitung von personenbezogenen Daten

Daten über Infektionen mit dem Coronavirus (COVID-19) und Daten über Verdachtsfälle zählen zu den sensiblen Daten (= die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Artikel 9 DSGVO) und unterliegen damit einem besonderen datenschutzrechtlichen Schutz. Die Verarbeitung dieser Daten ist gem. Art. 9 Datenschutz-Grundverordnung (DSGVO) grundsätzlich untersagt. Das Gesetz sieht jedoch Ausnahmen vor, wonach Gesundheitsdaten in jenem Ausmaß verwendet werden dürfen, welches notwendig ist, um die Verbreitung des Virus einzudämmen. Im Zusammenhang mit einer möglichen Infizierung mit Covid-19 kann die Verarbeitung personenbezogener Daten notwendig sein, weshalb folgende Ausnahmebestimmungen des Art. 9 Abs. 2 DSGVO zu tragen kommen:

- wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt (lit a);
- wenn die Verarbeitung der Daten für die Einhaltung arbeits- und sozialrechtlicher Pflichten (lit b) notwendig ist;
- wenn das Verarbeiten von Daten zum Zwecke der Gesundheitsvorsorge erforderlich ist (lit h).

Teilt ein Arbeitnehmer seinem Arbeitgeber freiwillig mit, dass eine bestätigte Infizierung durch COVID-19 oder entsprechende Symptome vorliegen, so ist der Arbeitgeber dem Gesetz nach verpflichtet, diese Informationen im Sinne seiner Fürsorgepflicht und zum Schutz anderer Mitarbeiter zu erheben und verarbeiten, um damit entsprechende Gesundheitsrisiken zu minimieren. Der Arbeitgeber hat jedoch nicht das Recht, die ihm bekanntgegebenen Informationen an andere Mitarbeiter oder Dritte weiterzugeben.

Maßnahmen bei Einführung von Homeoffice

- Angemessenes Schutzniveau für sensible Daten auch im Homeoffice
- Sichere Verbindung & Antivirus Programm sind unerlässlich
- Sichere Verwahrung von Betriebsgeheimnissen auch im Homeoffice durch Arbeitnehmer
- Sensible Daten und Betriebsgeheimnisse sind auch vor im gemeinsamen Haushalt lebenden Personen zu schützen
- Keine Weitergabe personenbezogener Daten
- Vorsicht bei privaten Kommunikationsmitteln (WhatsApp, Facebook, Instagram etc.)

Entsprechend des Grundsatzes der Datenminimierung hat der Arbeitgeber die Informationen so zu verarbeiten, dass sie nur für den angegebenen Zweck dienen, aber nicht darüber hinaus. Sofern die betroffene Person nicht ausdrücklich zustimmt, sind die personenbezogenen Daten anonym zu halten.

Innerhalb eines Betriebs hat der Arbeitgeber, sofern er Daten erhoben hat, entsprechende Datensicherungsmaßnahmen und Sicherheitsvorkehrungen zu treffen, um sicherzustellen, dass nur diejenigen Personen im Unternehmen Zugriff auf diese Daten haben, die zur Verarbeitung der Daten erforderlich sind. Die Verwendung der erhobenen Daten für andere Zwecke als der Gesundheitsvorsorge, der Eindämmung des Virus und der Heilbehandlung ist jedenfalls unzulässig. Darüber hinaus sind die erhobenen Daten, sobald sie für die Zweckerfüllung (spätestens nach Ende der Epidemie) nicht mehr notwendig sind, umgehend zu löschen.

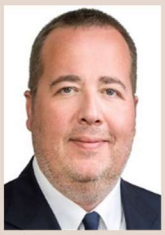
Datenschutz und Homeoffice

Arbeitgeber sind gemäß Art. 32 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie unterschiedlicher Eintrittswahrscheinlichkeiten und Schwere des Risikos, dazu verpflichtet, durch technische und organisatorische Maßnahmen ein dem Risiko angemessenes Schutzniveau sicherzustellen. Ferner hat der Arbeitgeber die Verantwortung für die Bereitstellung und Wartung aller vom Arbeitnehmer benötigten Arbeitsmaterialien. Um die Datensicherheit des Unternehmens zu schützen, sind zudem eine sichere Netzwerkverbindung (z.B. durch ein Virtual Private Network „VPN“) sowie die Installation eines geeigneten Antivirus-Programms unerlässlich.

Für den Arbeitnehmer gilt auch im Homeoffice die Pflicht, Datengeheimnisse, Betriebs- und Geschäftsgeheimnisse sicher zu bewahren.

In diesem Zusammenhang ist insbesondere bei Video- oder Telefonkonferenzen von der Weitergabe von personenbezogenen Daten sowie von Betriebs-und Geschäftsgeheimnissen, insbesondere über private

DIE AUTOREN



Dr. Peter Wagesreiter, LL.M.

M&A, Finance und Corporate Governance & Compliance

E: wagesreiter@hsp-law.at
W: www.hsp-law.at

Sebastian Borer, LL.M.

M&A, Finance und Governance & Compliance Corporate

E: borer@hsp-law.at
W: www.hsp-law.at

Tracking-App: Jeder Grundrechtseingriff muss nach dem Verhältnismäßigkeits-grundsatz in der jeweils gelindesten zum Ziel führenden Art vorgenommen werden.

Kommunikationsmittel (z.B. WhatsApp, Facebook, Instagram etc.), Abstand zu nehmen, da nicht sichergestellt werden kann, dass der ausgewählte Serviceanbieter die erforderlichen rechtlichen (gemäß DSGVO betreffend personenbezogener Daten und UWG betreffend Betriebs-und Geschäftsgeheimnisse) und technischen Erfordernisse erfüllt.

Problematisch stellt sich der Umgang mit Datenschutz sowie Betriebs- und Geschäftsgeheimnissen auch dann dar, wenn auf engem Raum gemeinsam mit einem Partner oder auch Kindern gearbeitet wird und allenfalls Dokumente ausgedruckt mit nach Hause genommen werden, wodurch für Unbefugte der Zugang zu Informationen geschaffen wird. Ist ein Ausdrucken von Dokumenten unvermeidbar, so hat der Arbeitgeber sicherzustellen, dass ausgedruckte Unterlagen entsprechend vernichtet werden.

Aufgrund der schnellen Umstellung des Bürobetriebs auf digitale Arbeit, insbesondere auf Homeoffice, ausgelöst durch die im Zusammenhang mit COVID-19 erlassenen Maßnahmen zur Verhinderung der Verbreitung von COVID-19, empfehlen wir die geschaffenen Homeoffice-Bedingungen auch rechtlich überprüfen zu lassen, um den Bestimmungen der DSGVO sowie gesetzlichen Regelungen zur Arbeitsplatz-Ausstattung gerecht zu werden und die Datensicherheit im Unternehmen zu gewährleisten.

Exkurs: (Verpflichtende) Tracking-App

Datenschutzrechtliche Problematiken bestehen derzeit auch im Zusammenhang mit der Einführung einer sogenannten „Tracking-App" (darunter fällt sowohl die Verwendung einer App am Smartphone als auch über einen elektronischen Schlüsselanhänger) zur Eindämmung des COVID-19-Virus. Auch hier kommt es zu einer Verwendung bzw. Verarbeitung von Daten über Infektionen mit dem Coronavirus (COVID-19).

Während die Verwendung bzw. Verarbeitung dieser „sensiblen" Daten im Rahmen der App mit Zustimmung des Betroffenen zulässig ist, würde eine gesetzliche Verpflichtung zur Verwendung der App einen massiven Eingriff in mehrere verfassungsrechtlich gewährleistete Grundrechte darstellen (Recht auf Datenschutz, Recht auf Privatleben, Recht auf Freizügigkeit, …).

Jeder Grundrechtseingriff muss nach dem Verhältnismäßigkeitsgrundsatz in der jeweils gelindesten zum Ziel führenden Art vorgenommen werden. Die gesetzlich vorgeschriebene Verwendung der App bzw. Standortüberwachung muss geeignet sein, ein legitimes Ziel zu erreichen.

Im gegenständlichen Fall ist fraglich, ob eine verpflichtende Tracking-App bzw. Standortüberwachung überhaupt geeignet ist, das legitime Ziel – die Verhinderung von weiteren Ansteckungen bzw. die Gesundheit der Bevölkerung zu schützen – zu erreichen. Zudem muss die Frage aufgeworfen werden, warum eine verpflichtende App bzw. eine Standortüberwachung das legitime Ziel besser erreicht als die gelinderen Mittel der Verpflichtung zum Tragen von Masken oder insbesondere die Verpflichtung zum Abstandhalten.

Für Rückfragen zu diesem Thema stehen wir Ihnen auch aktuell jederzeit gerne zur Verfügung.

INHALTSVERZEICHNIS

NACHSCHLAGEWERK

Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz (BGBl. II Nr. 98/2020)

Verordnung des Bundesministers für Soziales, Gesundheit, Pflege und Konsumentenschutz (BGBl. II Nr. 107/2020)