COVID-19: gli impatti sulla privacy e sulla tutela dei dati personali nei luoghi di lavoro.

Angesichts der sanitären Notlage, der sich die Welt in diesen Monaten gegenübersieht, ist es notwendig, die relevanten Aspekte im Zusammenhang mit dem Schutz personenbezogener Daten am Arbeitsplatz zu analysieren, sowohl unter Berücksichtigung der Klarstellungen des staatlichen Datenschutzbeauftragten vom 2. März 2020 als auch der Absichtserklärung zwischen Gewerkschaften und Unternehmensverbänden vom 14. März 2020 über Maßnahmen zur Eindämmung und Bekämpfung von COVID-19 am Arbeitsplatz.

Insbesondere ist es notwendig, das Gleichgewicht der verschiedenen im Raum stehenden Interessen zu beachten, und daher einerseits den Schutz der Gesundheit und das kollektive Interesse an der Erlangung von Namen, Nachnamen, Anwesenheit, Reisen, um die Verbreitung des Virus zu begrenzen, und andererseits das Recht auf Privatsphäre der vom Coronavirus Betroffenen in Einklang zu bringen, da eine mögliche Sammlung personenbezogener Daten sicherlich zu einer Verletzung dieses Rechts führen würde.

I. Mögliche Maßnahmen der Arbeitgeber

Der staatliche Datenschutzbeauftragte stellt mit der Stellungnahme vom 02. März 2020 zunächst klar, dass "Do-it-yourself"-Initiativen des Arbeitgebers verboten sind, und schließt insbesondere aus, dass der Arbeitgeber von vornherein und in verallgemeinerter und systematischer Weise Informationen über den Gesundheitszustand seiner Mitarbeiter im Zusammenhang mit Grippesymptomen und über die engsten und jedenfalls nicht beruflichen Kontakte sammeln darf. Die oben erwähnte Absichtserklärung erlaubt es dem Arbeitgeber jedoch, die Temperatur seiner Mitarbeiter zu messen, ohne die gesammelten Daten aufzuzeichnen, es sei denn, die Temperatur liegt über 37,5°; in diesem Fall ist es erlaubt, den Mitarbeiter zu identifizieren und ihm in einer mit Gründen versehenen Erklärung den Zugang zum Betrieb zu verweigern. Es ist zulässig, die Informationen über die Verarbeitung personenbezogener Daten gemäß Artikel 13 GDPR bereitzustellen, da das Protokoll die Möglichkeit vorsieht, dass die Informationen auch mündlich übermittelt werden können.

II. Pflichten der Mitarbeiter

Der staatliche Datenschutzbeauftragte hat weiterhin festgelegt, dass jeder Arbeitnehmer weiterhin verpflichtet ist, seinen Arbeitgeber über das Bestehen einer Gefährung für Gesundheit und Sicherheit am Arbeitsplatz zu informieren. Das bedeutet also, dass, wenn der Arbeitnehmer Symptome im Zusammenhang mit einer Coronavirusinfektion aufweist oder in den vorangegangenen 14 Tagen Gebiete mit epidemiologischem Risiko aufgesucht oder Kontakt mit infizierten Personen gehabt hat, derselbe Arbeitnehmer dem Arbeitgeber diese Informationen zur Verfügung stellen muss. Daher sollte es nach Ansicht des Datenschutzbeauftragten als zulässig angesehen werden, dass der Arbeitgeber seine Mitarbeiter einlädt, solche Informationen gegebenenfalls weiterzugeben. Das Unternehmen hat nämlich die Pflicht, seine Arbeitnehmer und diejenigen, die Zugang zum Unternehmen haben, über die Bestimmungen des Datenschutzbeauftragten auf solche eine Art und Weise zu informieren, die es für die geeignetste und wirksamste hält (z.B. durch Aushang von erläuternden Broschüren).

Der Datenschutzbeauftragte stellt überdies klar, dass die einzigen Stellen, die für die Beschaffung von Informationen über die typischen Symptome des Coronavirus und über die Kontakte und Bewegungen des Arbeitnehmers verantwortlich sind, die Mitarbeiter des Gesundheitswesens und des Zivilschutzes sind. Das Kommuniqué sieht auch vor, dass der Arbeitnehmer, eventuell auch über seinen Arbeitgeber, den zuständigen Gesundheitsdiensten die Daten einer Person, die im Verdacht steht mit dem Coronavirus infiziert zu sein mitteilen muss, falls dieser Arbeitnehmer bei der Durchführung von Aufgaben, die den Kontakt mit der Öffentlichkeit beinhalten, mit dieser "verdächtigen" Person in Kontakt gekommen ist.

III. Im Betrieb zu ergreifende Maßnahmen

Doch welche Sicherheits- und Organisationsmaßnahmen am Arbeitsplatz sind für den Datenschutz notwendig?

Die Absichtserklärung macht deutlich, dass es in erster Linie notwendig ist, die Verantwortlichen für die Datenverarbeitung zu

ernennen und zu instruieren. In Bezug auf Sicherheitsmaßnahmen ist es notwendig, auf Art. 25 GDPR zu verweisen, wo es heißt: "Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Maßnahmen, wie z.B. Pseudonymisierung, durchzuführen, um die Datenschutzgrundsätze, wie z.B. Minimierung, wirksam umzusetzen und die erforderlichen Garantien in die Verarbeitung zu integrieren, um die Anforderungen dieser Verordnung zu erfüllen und die Rechte der betroffenen Personen zu schützen", und in Bezug auf technische Maßnahmen nach Art. 32 GDPR

(a) die Pseudonymisierung und Verschlüsselung von persönlichen Daten;

(b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten dauerhaft zu gewährleisten;

(c) die Fähigkeit, die rechtzeitige Verfügbarkeit und den Zugang zu persönlichen Daten im Falle eines physischen oder technischen Zwischenfalls wiederherzustellen;

(d) ein Verfahren zur regelmäßigen Prüfung, Verifizierung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten"

IV. Insbesondere: das Homeoffice

Besondere Probleme ergeben sich im Zusammenhang mit dem Homeoffice, der in dieser Zeit auch nach den Anweisungen der Regierung weit verbreitet ist, und insbesondere mit dem Schutz personenbezogener Daten. Es ist unerlässlich sich auf bestimmte Aspekte zu konzentrieren, wie z.B. die Erstellung einer Unternehmenspolitik, in der der Arbeitgeber die Verhaltensrichtlinien für die Verwendung von Arbeitsmitteln, die Verwaltung von Passwörtern, die Installation von Antiviren-Software, die Nutzung von Internet und E-Mail, die Speicherung von Dateien und die Konsequenzen für den Arbeitnehmer im Falle der Verletzung von Pflichten und Verhaltensregeln festlegt; es ist auch unerlässlich, eine Folgenabschätzung zum Datenschutz vorzubereiten (Art. 35 DS-GVO), d.h. ein Verfahren, das ständig aktualisiert werden muss und das die Art, den Zweck und die Risiken der Datenverarbeitung im Unternehmen beschreibt, um die Risiken und die zu treffenden Sicherheitsmaßnahmen zu bewerten. Es ist notwendig, dem Arbeitnehmer die Datenschutzpolitik (Art. 13 DS-GVO) bezüglich der Verarbeitung seiner persönlichen Daten, die mit Hilfe der verwendeten Werkzeuge und der Software gesammelt wurden, zur Verfügung zu stellen, aus der sich die Möglichkeit der Kontrolle durch den Arbeitgeber ableiten lässt, sowie ein spezifisches Verfahren für den Fall einer Datenverletzung vorzusehen, wie es in den Art. 33 und 34 DS-GVO vorgesehen ist, da es notwendig ist, dass der Arbeitnehmer im Falle einer Datenverletzung im Rahmen seiner Arbeitstätigkeit den Arbeitgeber unverzüglich informiert.