Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

DSG-Info-Service

März 2020 Ausgabe Nr. 94

Sehr geehrter DSG-Paket-Kunde!
Sehr geehrter Leser!

Das Corona-Virus hat die wirtschaftliche Landschaft maßgeblich getroffen und wesentliche Auswirkungen auf das tägliche Leben.

In dieser Sonder-Information möchten wir Sie über die aktuelle Lage informieren und Antworten auf Fragen geben, die sich in dieser neuen Situation stellen.

1. Arbeitsrecht und Datenschutz

Darf ich meine Mitarbeiter nach der Erkrankung COVID-19 fragen und diese Daten verarbeiten?

Die DSGVO ermöglicht in dieser Ausnahmesituation die Erhebung von Gesundheitsdaten. Hierzu gelangt die Rechtsgrundlage des Art. 9 Abs. 2 lit. b DSGVO *[Verarbeitung zum Zwecke der Erfüllung arbeits- und sozialrechtlicher Pflichten]* zur Anwendung.

Dabei sind Fragen erlaubt wie beispielsweise nach der positiven Erkrankung oder zu konkreten Verdachtsmomenten aufgrund von bereits bestätigten Fällen oder dem Besuch von Risikogebieten.

Achtung: Mündliche Mitteilungen sind ebenso von dem Recht auf Geheimhaltung des § 1 Abs. 1 DSG umfasst wie schriftliche oder elektronische Informationen. Die Informationen dürfen nur zum Zweck der Gesundheitsprävention bzw. zum Schutz der übrigen Mitarbeiter verarbeitet werden. Sofern Sie mit Fragebögen oder Dateisystemen arbeiten, sind diese entsprechend dem hohen Schutzbedarf der Daten gesichert aufzubewahren und nach Erreichung des Zwecks (idR Verkündigung des Epidemie-Endes) zu vernichten.

Wie kann ich die übrigen Mitarbeiter schützen?

Als Arbeitgeber treffen Sie umfassende Fürsorgepflichten. Allerdings ist auch der Arbeitnehmer gefordert, Ihnen Umstände mitzuteilen, die das gegenseitige Arbeitsverhältnis betreffen. Ist ein Mitarbeiter positiv getestet worden oder besteht ein konkreter Verdachtsfall, so stellt seine weitere Tätigkeit am Arbeitsplatz ein Gesundheitsrisiko dar. Um weitere Mitarbeiter und sich selbst zu schützen, darf der Umstand einer (potenziellen) Erkrankung auf Grundlage von Art. 9 Abs. 2 lit. b DSGVO [*Verarbeitung zum Zwecke der Erfüllung arbeits- und sozialrechtlicher Pflichten*] verarbeitet werden.

Was muss ich als Arbeitgeber tun, wenn ich weiß, dass ein Mitarbeiter an COVID-19 erkrankt ist?

Die DSGVO erlaubt die Mitteilung an die jeweilige Bezirksverwaltungsbehörde (Gesundheitsamt) auf der Grundlage von Art. 9 Abs. 2 lit. i DSGVO [*Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit*] iVm § 2 Abs. 1 Epidemiegesetz.

Das Coronavirus ist eine anzeigepflichtige Krankheit iSd § 1 Abs. 1 EpidemieG. Arbeitgeber sind gem. § 5 Abs. 3 EpidemieG verpflichtet, relevante Auskünfte zur Erhebung des Auftretens der Krankheit zu erteilen. Laut dem aktuellen Informationsblatt der DSB ist das Corona-Virus als „Katastrophenfall" iSd § 10 DSG zu sehen, sodass die Übermittlung der rechtmäßig erhobenen Daten von Infizierten an Gesundheitsbehörden zulässig ist.

2. Home Office

Die aktuelle Situation hat viele Unternehmen gezwungen, die betriebliche Infrastruktur ins sog. „Home-Office" zu verlegen und Telearbeit anzuordnen. Da dies keine vollkommen neue Entwicklung ist, verfügen viele Unternehmen bereits über Richtlinien oder Dienstanweisungen für die Telearbeit. Oftmals ist auch eine Betriebsvereinbarung im Unternehmen mit Betriebsrat abgeschlossen worden, die die Inanspruchnahme von Telearbeit regelt.

a) Habe ich eine Richtlinie/Dienstanweisung oder Betriebsvereinbarung für Telearbeit/Home-Office?

Sofern Sie bereits dokumentierte Maßnahmen getroffen haben, sollte darin die rechtliche Absicherung für die Nutzung der betrieblichen Infrastruktur, einschließlich der Betriebsmittel (Dienst-Laptop/Handy), sowie für die Mitnahme und sichere Verwahrung von Dokumenten. die Geschäfts- und Betriebsgeheimnisse enthalten, geregelt werden. Die Pflichten der Mitarbeiter zur Absicherung ihres Heimarbeitsplatzes müssen ebenso umfasst sein wie die Möglichkeiten des Unternehmens zur Kontrolle oder sogar Sperre beim Auftreten von Sicherheitsproblemen. Soweit erforderlich, sind auch Arbeits- und Bereitschaftszeiten und die Pflichten zur Erfassung der Arbeitszeit zu berücksichtigen.

Abhängig vom Umfang der Regelungen muss für solche Maßnahmen entweder eine Richtlinie in Kraft gesetzt oder eine Betriebsvereinbarung abgeschlossen werden. Falls Ihr Unternehmen noch nicht über eine entsprechende Richtlinie oder Betriebsvereinbarung verfügt, können wir Sie aufgrund unserer langjährigen Erfahrung schnell und effizient unterstützen.

b) Welche technischen Maßnahmen kann ich für mein Unternehmen wählen?

Das hängt von der Grundanlage Ihrer IT-Infrastruktur ab. Es muss zwischen lokaler und Cloud-Infrastruktur unterschieden werden:

- Lokale Infrastruktur

Sollten Sie Ihre IT-Anlagen im eigenen Unternehmen betreiben, das heißt Informationen mit eigenen Servern und Anwendungen verarbeiten und auf Firmen-Laufwerken speichern, müssen sich alle Telearbeiter über verschlüsselte Verbindungen (VPN-Tunnel) mit dem Unternehmen verbinden. Zusätzlich muss eine sichere Lösung für den Fernzugriff auf Unternehmenscomputer und -Anwendungen eingesetzt werden. Für diesen Zweck wird meistens Citrix- oder MS Remotedesktop-Software verwendet.

Sie können mit dieser Variante vollständig das Speichern auf privaten Clients ersetzen und reduzieren damit auch das Risiko, dass Schadsoftware in Ihr Unternehmen eingeschleppt wird. Lösungen dieser Art lassen sich sehr gut absichern und ermöglichen es, ohne jede Einschränkung von zu Hause weiterzuarbeiten. Sie lassen sich jedoch nicht ad hoc für

ein komplettes Unternehmen einrichten, sondern benötigen etwas Vorbereitung und Planung.

- Cloud-Lösungen

Wenn Sie Ihre Anwendungen teilweise oder vollständig in die Cloud verlegt haben, können Sie auch auf diese Art Ihren Mitarbeitern den Zugriff von zu Hause auf die Arbeitsmittel ermöglichen. Die entsprechenden Sicherheitsvorkehrungen sollten bei seriösen Cloud-Dienstleistern bereits vorhanden sein. Wenn für diesen Zweck bisherige Einschränkungen, zB bei den erlaubten Netzwerkverbindungen, aufgehoben werden müssen, müssen Sie zuvor das Risiko prüfen.

Probleme können auftreten, wenn die eigenen Kernanwendungen nicht als Cloud-Anwendung verfügbar sind oder wenn besonders schutzbedürftige Daten bisher auf eigenen Servern gespeichert werden. Überstürzte Lösungsversuche sind zu vermeiden: Ein Data Breach ist auch in der aktuellen Ausnahmesituation weiterhin strafbar und kann darüber hinaus zu Vertrauensverlust mit entsprechenden wirtschaftlichen Auswirkungen führen.

Außerdem sind keineswegs alle Cloud-Anwendungen für eine geschäftlich-kommerzielle Nutzung geeignet oder zugelassen. Oft schlagen Mitarbeiter Lösungen vor (oder setzen sie sogar ohne vorherige Rücksprache ein), die ihnen aus ihrem privaten Gebrauch vertraut, aber ausschließlich für den Consumer-Bereich gedacht sind. Wenn Firmengeheimnisse oder personenbezogene Daten über derartige Produkte verarbeitet oder ausgetauscht werden, kann es zu erheblichen rechtlichen oder wirtschaftlichen Problemen kommen. Die Bedürfnisse der Mitarbeiter müssen berücksichtigt werden, um diesen Entwicklungen zuvorzukommen. Gleichzeitig muss aber klar sein, dass ausschließlich geprüfte und zugelassene Software zur Verarbeitung von Unternehmensdaten eingesetzt werden darf.

Die Auswahl einer geeigneten Cloud-Lösung sollte zusätzlich auch Faktoren wie Verfügbarkeit, Lizenz-Kapazitäten sowie Firmensitz und Betriebsort berücksichtigen: Aus datenschutzrechtlicher Sicht ist der Betrieb im EWR/EU oder einem sicheren Drittland (Privacy Shield für die USA oder Kanada etc.) zulässig. Für die Verarbeitung von Geschäftsgeheimnissen und Daten mit hohem Schutzbedarf ist ein Betreiber, der seinen Firmensitz innerhalb der EU hat, dennoch grundsätzlich vorzuziehen.

c) Welche Sicherheitsmaßnahmen muss ich treffen?

Die Wahl der erforderlichen Sicherheitsmaßnahmen hängt stark von den eingesetzten Methoden ab. Aus datenschutzrechtlicher Sicht lassen sich aber einige allgemeine Aussagen treffen:

- Koordinieren Sie intern den Einsatz von Home Office-Methoden mit Ihrem IT-Management, Ihrem Informationssicherheitsbeauftragten, Ihrem Datenschutzbeauftragten und dem Betriebsrat (so vorhanden). Prüfen Sie die jeweiligen Vorschläge und Stellungnahmen und entscheiden Sie auf der Basis des erwarteten Risikos. Dokumentieren Sie die Entscheidungen zum Nachweis Ihrer Sorgfalt und zur Erfüllung Ihrer Rechenschaftspflicht. Binden Sie die Schlüsselfunktionen in die einzelnen Entscheidungen ein und berücksichtigen Sie Ihre eigene Infrastruktur.
- Achten Sie darauf, keine Consumer-Anwendungen aus der Cloud für Geschäftszwecke zu nutzen, um zu verhindern, dass unkontrolliert Betriebsgeheimisse oder personenbezogene Daten abfließen. Zudem ist zu beachten, wo der Dienstleister seine Anwendungen betreibt (zB in einem Drittland), da dies ggf. eine datenschutzrechtliche Zusatzvereinbarung (Standardvertragsklauseln) erfordert.
- Nützen Sie die Gelegenheit, um Ihre Mitarbeiter für Fragen der Informationssicherheit

und des Datenschutzes zu sensibilisieren. Gerade in der Situation im Home-Office ist es unbedingt erforderlich, dass Ihre Mitarbeiter selbstständig sichere Entscheidungen treffen. Das betrifft einerseits die Sicherheit des Heimarbeitsplatzes, der vor unbefugten Zugriffen und Einsichten zu schützen ist (auch vor Familienmitgliedern oder Mitbewohnern), andererseits aber auch Übermittlungen und Telefonate, über die Ihre Mitarbeiter jetzt in Abwesenheit von Kollegen und Vorgesetzten entscheiden müssen. Sie können sie dabei unterstützen, indem Sie gezielt und regelmäßig auf Bedrohungen hinweisen. Sie können auch eine Anlaufstelle bereitstellen, die aktuelle Sicherheitsanfragen beantwortet und die Antworten zu häufig gestellten Fragen an alle anderen Mitarbeiter weiterreicht.

- Bei einem umfassenden Einsatz von Home Office-Anwendungen treffen das Unternehmen wesentliche Fragen zu Datenlöschungen, Datenschutzverletzungen (Verlust oder Missbrauch von Daten) sowie zur Integration der Anwendungen in die Betriebssicherheit der IT-Systeme (Backups und Synchronisation der Daten).

d) Welche Rahmenbedingungen gelten im Home-Office?

Sofern Sie eine Betriebsvereinbarung zur Telearbeit im Betrieb haben, muss sie zu ihrer Geltung für die Belegschaft in ihrem Anwendungsbereich bereitgestellt werden. Selbstverständlich müssen Sie auch eine eventuelle Richtlinie an die Mitarbeiter kommunizieren. Wenn diese Dokumente schon länger bestehen, sollten die Mitarbeiter nochmals gezielt darauf hingewiesen werden, sodass bei eventuellen Streitfällen Unkenntnis nachweislich ausgeschlossen werden kann.

Bitte beachten Sie, dass Sie weiterhin Verantwortlicher iSd Art. 4 Z 7 DSGVO und damit für alle im Home-Office getätigten Datenverarbeitungen Ihrer Mitarbeiter verantwortlich sind. Dazu gehören auch Data Breaches, die nach wie vor der Datenschutzbehörde zu melden sind, sowie die allgemeinen Grundsätze der Datenverarbeitung des Art. 5 DSGVO und technischen und organisatorischen Sicherheitsmaßnahmen des Art. 32 DSGVO.

Folgende Eckpfeiler sind für den Einsatz von Home-Office zu beachten:

- Bereitstellung der notwendigen Betriebsmittel, nach Bekanntgabe durch die Mitarbeiter: Haben Ihre Mitarbeiter keine ausreichenden Ressourcen für die Arbeit im Home-Office, müssen Sie diese als Arbeitgeber kostenlos bereitstellen. Ein Kostenersatz für die Nutzung eigener Betriebsmittel ist möglich und sollte vorab geregelt werden.
- Richten Sie eine Anlaufstelle in der IT und Personalabteilung ein, die Anfragen zu technischen Anforderungen und Problemen entgegennimmt.
- Aus arbeitsrechtlicher Sicht ist es empfehlenswert, die Telearbeit anzuordnen. Führungskräfte sind angehalten, betriebskritisches Personal zu identifizieren und allfällig notwendige Anwesenheiten zu koordinieren. Mit Telearbeit ersetzen Sie die Präsenzarbeit im Ausmaß der angeordneten Dauer und Umfang. Ein Verstoß gegen diese Anordnung führt zu einer Missachtung einer Weisung und kann die Kündigung aus in der Person liegenden Gründen zur Konsequenz haben. Weiters kann eine Weigerung zur Telearbeit nach angeordneter Weisung eine Entlassung aus wichtigen Gründen darstellen.
- Achten Sie darauf, dass die Telearbeitszeit, sofern möglich, durch den Mitarbeiter in den entsprechenden Zeiterfassungssystemen vermerkt wird, oder stellen Sie eine geeignete Erfassungsmöglichkeit zur Verfügung. Telearbeitszeit wird wie eine Präsenzarbeitszeit gewertet. Das Empfangen, Senden oder Bearbeiten von elektronischen Nachrichten erfolgt zeitlich unbeschränkt, es sollte jedoch von keinem

Mitarbeiter eine zeitliche Dauerverfügbarkeit erwartet werden.

- Vertrauliche Informationen wie Passwörter und Geschäftsinterna sind durch die Mitarbeiter so zu schützen, dass Dritte (einschließlich Familienmitglieder oder im Haushalt lebende Personen) keinen Zugriff darauf haben.
- Das Führen von Remotekonferenzen sollte zur Schonung der Betriebsmittel und der Netzwerkinfrastruktur möglichst ohne Anwendung von Videotelefonie erfolgen. Falls dies dennoch notwendig sein sollte, muss eine Anwendung gewählt werden, die allen Anforderungen des Datenschutzes und der IT-Sicherheit entspricht. Werden die Bild- und Tondaten nicht nur übertragen, sondern zusätzlich auch aufgezeichnet, muss dafür in jedem Fall ein eigenes Verarbeitungsverzeichnis erstellt werden. Eventuell muss auch eine entsprechende Betriebsvereinbarung abgeschlossen werden.

3. Weiterführende Links

Informationen des A-SIT zu Home Office in Zeiten der Corona-Situation: https://www.onlinesicherheit.gv.at/service/news/532326.html

Aktion it-safe der Bundessparte Information und Consulting, insb. Sicherheitshandbücher: https://www.wko.at/site/it-safe/start.html?shorturl=it-safeat

Aktuelle Warnungen des BKA vor Online-Betrug: https://bundeskriminalamt.at/news.aspx?id=7745347A7971512F6968343D

Informationsblatt der Datenschutzbehörde „Datensicherheit und Home-Office“: https://www.dsb.gv.at/documents/22758/23115/Informationsblatt_der_Datenschutzbehoerde_Datensicherheit_und_Home-Office.pdf

4. Verschiebung der DSGVO-Praxisseminare

Angesichts der aktuellen Situation sehen wir uns gezwungen, die für den 21. und 22. April 2020 angesetzten Seminare zu verschieben. Die **neuen Termine** sind:

„**Rechtsentwicklung und Best Practices**“

mit dem rechtlichen Schwerpunkt findet am **23. Juni 2020** statt.

Das Praxisseminar

„Praxisnahe Updates zu Datenschutz und IT-Sicherheit“

mit Schwerpunkt auf technische Umsetzungsmaßnahmen, Erläuterungen zu TOM und offene Fragen der Informationssicherheit findet nun am **24. Juni 2020** statt.

Veranstaltungsort ist weiterhin das Hotel de France, Schottenring 3, 1010 Wien.

Bestehende Anmeldungen können kostenlos storniert werden bzw. gelten auch für die neuen Termine weiter.

Sollten Sie eine Inhouse-Schulung wünschen, können Sie sich jederzeit an uns wenden.

Nähere Informationen finden Sie unter www.secur-data.at.