Pressemitteilung

EU-DSGVO 26. Januar 2021

Homeoffice: Das ist beim Datenschutz zu beachten

München. In der aktuellen Pandemiesituation steht das Arbeiten im Homeoffice wieder verstärkt im Fokus. Unternehmen sehen sich aufgefordert, ihren Mitarbeitenden das Arbeiten von zuhause zu ermöglichen, wo immer dies betrieblich machbar ist. TÜV SÜD erklärt, was dabei zu beachten ist, um beim Datenschutz auf der sicheren Seite zu sein.

Zu Beginn der Pandemie mussten viele Mitarbeitende oft sehr kurzfristig ihren Arbeitsplatz ins Homeoffice verlagern. In dieser für alle Beteiligten neuen Situation wurde viel improvisiert. Inzwischen ist klar: Das Homeoffice wird auch langfristig eine wichtige Rolle in unserer Arbeitswelt einnehmen. Unternehmen sollten deshalb ihre Arbeitsprozesse so gestalten, dass sie auch beim mobilen Arbeiten weiterhin die seit Mai 2018 geltenden Anforderungen der Datenschutzgrundverordnung (EU-DSGVO) bei der Verarbeitung personenbezogener Daten einhalten.

„Bisher gab es nur wenige Bußgelder. Aber die Coronakrise darf mittlerweile kein Grund mehr sein, die Anforderungen der EU-DSGVO zur Datenverarbeitung nicht einzuhalten, wenn von zuhause gearbeitet wird“, erklärt Mareike Vogt, Fachexpertin für Datenschutz TÜV SÜD. „Unternehmen sollten ihre technischen und organisatorischen Maßnahmen (TOM) entsprechend für eine rechtskonforme Verarbeitung von personenbezogenen Daten auch an Heimarbeitsplätzen anpassen. Kleinere Unternehmen mit wenig Ressourcen sollten dabei im Zweifel auch die Hilfe unabhängiger externer Experten nutzen, bevor sie das Risiko von Bußgeldern oder eines Imageschadens eingehen.“

Folgende Punkte zum Datenschutz sollten Unternehmen und Mitarbeitenden bei der Arbeit im Homeoffice beachten:

- **Sichere IT-Infrastruktur**
  Dem Arbeitnehmer sollten betriebliche Arbeitsmittel zur Verfügung gestellt werden, mit denen er sich ins Unternehmensnetz einwählen kann. Idealerweise handelt es sich dabei um ein in sich geschlossenes Virtual Private Network (VPN). Falls im Einzelfall ein Mitarbeiter doch sein

eigenes Gerät nutzen muss, um zu arbeiten, sollten auch hier entsprechende Maßnahmen getroffen werden.

- **Schulungen sensibilisieren gegen Phishing**
  Die Angriffsfläche für Phishingattacken wächst, sobald vermehrt im Homeoffice gearbeitet wird. Für den verantwortungsvollen Umgang mit sensiblen Daten sollten daher sämtliche Mitarbeiter verstärkt gegen solche Bedrohungen geschult werden.

- **Vereinbarungen zum Homeoffice treffen**
  Mit Mitarbeitern, die zeitweise von zuhause arbeiten, sollte eine Vereinbarung zur künftigen Arbeit im Homeoffice getroffen werden. Darin müssen im Einzelfall zutreffende Pflichten und vereinbarte Schutzvorkehrungen dokumentiert werden. Um dies datenschutzrechtlich von Anfang an sicher zu gestalten, sollte eine solche Regelung am besten von Beginn an getroffen und unterschrieben werden oder dies schnellstmöglich nachgeholt werden. Neben allgemeinen Maßnahmen zum Schutz, kann in einer solchen Vereinbarung auch ein Kontrollrecht des Arbeitgebers über den bestehenden Heimarbeitsplatz vereinbart werden.

- **Private und geschäftliche Daten trennen**
  Private und geschäftlichen Daten sollten getrennt sein. Auch hier sollten am besten alle Maßnahmen individuell innerhalb einer getroffenen Vereinbarung dokumentiert werden.

- **Regeln für Auftragsdatenverarbeitung beachten**
  Verarbeitet ein Unternehmen für ein anderes im Auftrag personenbezogene Daten, muss weiterhin beachtet werden, was innerhalb des Auftragsverarbeitungsvertrags vereinbart wurde – unter anderem die technischen und organisatorischen Maßnahmen (TOM) dürfen auch in solchen Situationen nicht unterschritten werden.

- **Kontrolle im Homeoffice: Was ist erlaubt?**
  Persönliche Kontrollbesuche sind nur erlaubt, wenn der Besuch vorher abgesprochen und nicht bloß angekündigt wurde. Keylogger-Software, die jeden Tastaturanschlag speichert und den Bildschirm hin und wieder fotografiert ist ebenfalls nur erlaubt, wenn ein konkreter Anlass vorliegt und der Einsatz der Software kommuniziert wurde. Zugriff auf geschäftlichen E-Mail-Verkehr darf der Chef immer einfordern; sind E-Mails jedoch durch den Betreff bereits deutlich als privat erkenntlich, dürfen diese auch bei Verbot der E-Mail-Privatnutzung nicht einfach so gelesen werden. Eine Kontrolle, ob private Mails verschickt wurden, ohne Einsicht, ist jedoch

möglich. Ebenso möglich ist es, den Browser-Verlauf des Dienst-Laptops auszuwerten – nicht jedoch des privaten Computers. Programme, wie z.B. Microsoft Teams zeigen zudem an, wer gerade online ist. In jedem Fall ist bei solchen Maßnahmen der Betriebsrat und der Datenschutzbeauftragte mit einzubeziehen.

„Letzten Endes zeigen diese Punkte deutlich, dass im besten Fall eine schriftliche Vereinbarung zwischen den Mitarbeitern und der Firmenführung getroffen wird, in der alle Aufgaben, Kontroll-Möglichkeiten und sonstigen Regularien festgelegt werden, um Klarheit zu schaffen“, sagt Mareike Vogt. „Unabhängige Experten können auch dabei unterstützen.“ Mehr Informationen über die Leistungen von TÜV SÜD im Bereich Datenschutz sind verfügbar unter: https://www.tuvsud.com/de-de/dienstleistungen/cyber-security/datenschutz.

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuvsud.com Internet www.tuvsud.com/de