1437/A(E) XXVII. GP

Eingebracht am 24.03.2021

Entschließungsantrag

der Abgeordneten Mag. Christian Drobits,

Genossinnen und Genossen

betreffend „Datensicherheit sowie Daten- und Geschäftsgeheimnisschutz im Homeoffice“

Die Corona-Krise hat Veränderungen in der Arbeitswelt deutlich beschleunigt: Homeoffice ist mittlerweile gekommen, um zu bleiben.

Der Nationalrat hat Ende Februar den steuerrechtlichen Teil und im März den arbeits- und sozialversicherungsrechtlichen Teil eines Homeoffice-Pakets beschlossen. Es ist sehr zu begrüßen, dass dank der umfangreichen Vorarbeiten der Sozialpartner*innen nun endlich klare Spielregeln für das Homeoffice gelten.

Im Bereich Datensicherheit sowie Datenschutz und Geschäftsgeheimnisschutz im Homeoffice – zum Beispiel zum Schutz vor Schadprogrammen (z.B. Emotet) – gibt es noch einige offene Fragen und Defizite, die überhaupt erst geregelt werden müssen.

Grundsätzlich gelten zwar sämtliche datenschutzrechtliche Regelungen (DSGVO, DSG) sowie die innerbetrieblich abgeschlossenen Regelungen auch im Homeoffice und müssen von Arbeitgeber*innen und Arbeitnehmer*innen eingehalten werden. Darunter fallen auch die Datensicherheitsmaßnahmen und die Gewährleistung des Geheimnisschutzes (besonders der Geschäftsgeheimnis-Schutz). Dabei muss im Homeoffice auch eine digitale Kontrolle des heimarbeitenden Arbeitnehmers durch den Arbeitgeber verhindert werden.

Datensicherheit und damit auch der Schutz vor Cyberangriffen stellt für alle Parteien im Arbeitsverhältnis eine hohe Herausforderung dar, wobei die generelle technische Absicherung durch die Arbeitgeberseite zu erfolgen hat und gewährleistet werden muss. Cyberkriminelle versuchen laufend Firmennetzwerke zu infiltrieren, um einen Zugriff auf die Firmen- und Geschäftsdaten zu bekommen. Es kommt dabei wie öffentlich bekannt gewordene Fälle zeigten, zu Datendiebstahl, Datenmanipulation und Datenmissbrauch.

Arbeitsmittel, die im Homeoffice vom Arbeitgeber bereitgestellt werden, müssen mit entsprechenden Sicherheitssystemen ausgestattet werden. Zusätzlich bedarf es regelmäßiger Anweisungen (Policies, Leitlinien etc.) und Unterweisungen sowie Schulungen für die Arbeitnehmer*innen, wie der Schutz von personenbezogenen Daten sowie auch der Schutz von Firmen- und Geschäftsdaten im Homeoffice zu gewährleisten ist (siehe z.B. das Informationsblatt der Datenschutzbehörde zu Datensicherheit und Home Office, https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html#Frage_14).

Problematischer ist es, wenn private Geräte der Arbeitnehmer*innen im Homeoffice zum Einsatz kommen („bring your own device“, BYOD): Der Arbeitgeber ist und bleibt der alleinige Verantwortliche nach der DSGVO. Daher muss es gerade in diesen Fällen firmeninterne Anweisungen (Policies, Leitlinien etc.) und Unterweisungen sowie Schulungen für die Arbeitnehmer*innen geben, wie der Schutz dieser Daten auch bei der Verwendung privater Geräte zu gewährleisten ist.

Noch schwieriger ist der Umgang mit den von der DSGVO geforderten technischen Sicherheitsmaßnahmen. Darunter fallen die Einhaltung der technischen Sicherheitsstandards, der gesicherte Datentransfer, die Datenlöschung und die Verwendung einer entsprechenden Infrastruktur des Arbeitgebers zum sicheren Zugriff auf das Firmennetz. Dies erfordert auch eine regelmäßige Wartung und Überprüfung der Sicherheitsstandards (ISO Norm 27701). Eine Zertifizierung dieser Standards ist wesentlicher Teil eines verantwortungsvollen betriebsinternen Risikomanagements. Schließlich muss zudem klar sein, dass bei der Verarbeitung von gewissen sensiblen Datenkategorien jedenfalls das Equipment vom Dienstgeber zur Verfügung zu stellen ist.

Unzureichende Maßnahmen zur Datensicherheit bei der Bearbeitung unternehmensbezogener Dokumente auf privaten Endgeräten können bei einem Hacker- oder Phishing-Angriff dazu führen, dass über das private Endgerät das Unternehmensnetzwerk und die damit verbundenen Endgeräte und Speicherorte kompromittiert und auf Firmendaten zugegriffen werden kann, die zu enormen Schäden führen können.

Die unterfertigten Abgeordneten stellen daher folgenden

Entschließungsantrag

Der Nationalrat wolle beschließen:

„Der Bundesminister für Arbeit wird aufgefordert, die Regelungen zur Datensicherheit sowie zum Daten- und Geschäftsgeheimnisschutz im Homeoffice zu evaluieren und dem Nationalrat bis spätestens 1.9.2021 eine Regierungsvorlage zu übermitteln, die eine Präzisierung eines Risikomanagementsystems (Datensicherheit) sowie spezielle Regelungen zum Daten- und Geschäftsgeheimnisschutz für die Arbeit im Homeoffice enthält und dabei u.a. folgende Aspekte berücksichtigt:

Besonderes Augenmerk ist bei der Erstellung des Gesetzentwurfes auf ein angemessenes Schutzniveau beim Einsatz von BYOD-Konzepten im Homeoffice zu

legen. Hier soll eine Festlegung bzw. Bekräftigung der datenschutzrechtlichen Verantwortung des Arbeitgebers (Art. 4 Z 7 DSGVO) erfolgen. Darüber hinaus wären spezielle Maßnahmen zur Gewährleistung der Datensicherheit (Art.32 DSGVO) vorzusehen.

Die Sicherheitsanforderungen und Sicherheits-Maßnahmen im Homeoffice sind regelmäßig zu überprüfen (Sicherheits-Updates) und gegebenenfalls zu evaluieren.

Sicherzustellen ist, dass erhöhte Datensicherheitsanforderungen nicht zu verstärkten/unverhältnismäßigen Verhaltens- und Leistungskontrollen führen dürfen. Die Privatsphäre der Arbeitnehmer*innen im Homeoffice, also in ihren privaten Räumlichkeiten, muss gewährleistet sein.

In diesem Sinn soll auch die Einführung und Verwendung von Maßnahmen und technischen Systemen zur Kontrolle von Arbeit im Homeoffice, welche die Menschenwürde berühren, als unzulässig normiert werden.

Unter Nutzung der Öffnungsklausel des Art. 88 Abs. 1 DSGVO soll zudem ein eigenes Beschäftigtendatenschutzrecht – unter Berücksichtigung der besonderen Erfordernisse im Homeoffice – geschaffen werden.“

Zuweisungsvorschlag: Ausschuss für Arbeit und Soziales