1338 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP

Bericht

des Ausschusses für Arbeit und Soziales

über den Antrag 1437/A(E) der Abgeordneten Mag. Christian Drobits, Kolleginnen und Kollegen betreffend "Datensicherheit sowie Daten- und Geschäftsgeheimnisschutz im Homeoffice"

Die Abgeordneten Mag. Christian **Drobits**, Kolleginnen und Kollegen haben den gegenständlichen Entschließungsantrag am 24. März 2021 im Nationalrat eingebracht und wie folgt begründet:

„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 Horne 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.“

Der Ausschuss für Arbeit und Soziales hat den gegenständlichen Entschließungsantrag in seiner Sitzung am 3. Februar 2022 in Verhandlung genommen. An der Debatte beteiligten sich außer dem Berichterstatter Abgeordneten Mag. Christian **Drobits** die Abgeordnete Bettina **Zopf**.

Bei der Abstimmung fand der gegenständliche Entschließungsantrag der Abgeordneten Mag. Christian **Drobits**, Kolleginnen und Kollegen nicht die Zustimmung der Ausschussmehrheit (**für den Antrag:** S, F, **dagegen:** V, G, N).

Zur Berichterstatterin für den Nationalrat wurde Abgeordnete Bettina **Zopf** gewählt.

Als Ergebnis seiner Beratungen stellt der Ausschuss für Arbeit und Soziales somit den **Antrag**, der Nationalrat wolle diesen Bericht zur Kenntnis nehmen.

Wien, 2022 02 03

Bettina Zopf	**Josef Muchitsch**
Berichterstatterin	Obmann

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2022-02-11T11:53:22+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	