
5504/J XXVII. GP

Eingelangt am 24.02.2021

Dieser Text wurde elektronisch übermittelt. Abweichungen vom Original sind möglich.

Anfrage

der Abgeordneten Mag. Christian Drobis,
Genossinnen und Genossen
an die Bundesministerin für Justiz bzw. den Bundesminister für Justiz

**betreffend Homeoffice im Spannungsverhältnis zu Datenschutz und
Datensicherheit**

Am 16. Februar 2021 ist das Homeoffice-Paket in Begutachtung gegangen. Der Begutachtungszeitraum beträgt insgesamt nur 3 Tage, was eine ernsthafte Begutachtung verunmöglicht. Es fällt auf, dass zwar Regelungen zur digitalen Infrastruktur für die Ausübung des Homeoffice vorgesehen sind, aber keine Bestimmungen zum Datenschutz (Datengeheimnis) oder zur Datensicherheit (Sicherheit personenbezogener Daten) beinhaltet sind, obwohl von IT-Experten und Kriminologen „Homeoffice“ als enormer Risikofaktor gesehen wird. Angriffe auf die IT-Infrastruktur nehmen von Jahr zu Jahr zu.

Diese Angriffe haben meist gravierende ökonomische und technische Folgen nach sich gezogen. Mit Homeoffice wird das Sicherheitsrisiko für das Unternehmen noch größer (z. B. Phishing-Attacken). Daher sind bei Homeoffice neben allgemeinen technisch organisatorischen Maßnahmen spezielle Datensicherheitsmaßnahmen notwendig.

Die unterzeichneten Abgeordneten stellen daher nachstehende

Anfrage:

1. Wann wurden Sie und Ihr Ressort von der Absicht, Homeoffice-Regelungen vorzubereiten, informiert?
2. Welche schriftliche Stellungnahme wurde von Ihrem Ressort aus der Sicht des Datenschutzes, für den Sie laut Bundesministeriengesetz die Verantwortung tragen, abgegeben?
3. Wie und wann wurde Ihr Ressort, insbesondere die Stabsstelle Datenschutz in die Vorbereitung dieses Gesetzespaketes eingebunden?

4. Warum wurde im Entwurf auf konkrete Regelungen zum Datenschutz und zur Datensicherheit (im Sinne von Art. 32 DSGVO) verzichtet?
5. Welche speziellen Regelungen sowie technisch organisatorische Maßnahmen wären aus Ihrer Sicht für Homeoffice notwendig, um Rechtsunsicherheiten im Bereich des Datenschutzes und der Datensicherheit zu verhindern und Sicherheitsprobleme zu verhindern und auszuschließen?
6. Welche Regelungen wären sinnvoll, um auch im Homeoffice höchstmöglichen Datenschutz und höchstmögliche Datensicherheit (siehe Art. 32 DSGVO) zu garantieren?
7. Welche Gefahren/Risiken können aus der Sicht des Datenschutzes durch Homeoffice-Lösungen entstehen, bei welchen personenbezogene Daten anfallen oder bearbeitet werden?
8. Welche Gefahren/Risiken können aus Sicht der Datensicherheit durch Homeoffice-Lösungen entstehen?
9. Welche dieser Gefahren/Risiken sind dem Ressort bereits bekannt geworden? Welche Probleme wurden von betroffenen Unternehmen direkt an das Ressort herangetragen?
10. Wie viele Strafanzeigen wurden diesbezüglich in den letzten 5 Jahren erstattet (bitte um Aufschlüsselung auf die jeweiligen Jahre)?
11. Welche Haftungsprobleme können im Rahmen von Homeoffice durch Schäden an der digitalen Infrastruktur des Unternehmens (z. B. durch Hacking) entstehen, wenn digitale Infrastruktur oder/und Arbeitsmittel vom Dienstgeber zur Verfügung gestellt wurden und Schäden aber vom Dienstnehmer zu verantworten sind?
12. Wie sieht die Haftungssituation aus, wenn die Arbeitsmittel im Eigentum des Arbeitnehmers stehen - auch privat verwendet werden - und Schäden von diesem zu verantworten sind? Spielt dabei die überwiegende Nutzung des Arbeitsmittels für dienstliche Zwecke eine Rolle?
13. Wie ist die Haftungssituation bei Schäden an dieser digitalen Infrastruktur, die durch im Haushalt wohnhafte Ehepartner/Lebensgefährten, Kinder, Haustiere oder Besucher entstehen?
14. Wie werden Sie den Abschluss von echten Betriebsvereinbarungen für Homeoffice-Lösungen unterstützen?