Republik Österreich
Datenschutzbehörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152 302563

E-Mail: dsb@dsb.gv.at

GZ: D055.408
2021-0.118.268

Sachbearbeiterin: Mag. Anna MICHELITSCH

Präsidium des Nationalrates

per E-Mail: begutachtungsverfahren@parlament.gv.at

Betrifft: **Stellungnahme der Datenschutzbehörde zum do. Entwurf eines Bundesgesetzes, mit dem das Arbeitsvertragsrechts-Anpassungsgesetz, das Arbeitsverfassungsgesetz, das Dienstnehmerhaftpflichtgesetz, das Arbeitsinspektionsgesetz 1993, das Allgemeine Sozialversicherungsgesetz, das Beamten-Kranken- und Unfallversicherungsgesetz und das Einkommensteuergesetz 1988 geändert werden (Homeoffice Maßnahmenpaket 2021), GZ: 2021-0.113.237**

Die Datenschutzbehörde wurde mit der im Betreff genannten GZ zur Stellungnahme eingeladen und nimmt aus Sicht ihres Wirkungsbereiches wie folgt Stellung:

Zu Artikel 1 Z 1 (§ 18c AVRAG):

Abs. 3 leg. cit. sieht vor, dass die Arbeitgeberin oder der Arbeitgeber die für das regelmäßige Arbeiten im Homeoffice gegebenenfalls erforderlichen digitalen Arbeitsmittel bereitzustellen hat. Davon kann durch Vereinbarung abgewichen werden, sodass ausnahmsweise digitale Arbeitsmittel vom Arbeitnehmer selbst bereitgestellt werden („bring your own device“).

Die letztgenannte Konstellation wirft jedenfalls die Frage auf, wer diesfalls für die erforderlichen Datensicherheitsmaßnahmen nach Art. 32 DSGVO Sorge zu tragen hat. Es ist nämlich nicht ausgeschlossen, dass Arbeitnehmer verpflichtet sind, sich mittels privater Endgeräte über eine Fernverbindung in das Unternehmensnetzwerk einzuwählen. Jedenfalls ist davon auszugehen, dass unternehmensbezogene Dokumente auf privaten Endgeräten bearbeitet und ggf. versendet werden. Unzureichende Datensicherheitsmaßen können diesfalls dazu führen, dass über das private Endgerät das Unternehmensnetzwerk und die damit verbundenen Endgeräte und Speicherorte kompromittiert werden (z.B. durch einen Hackerangriff).

Da die Einhaltung der erforderlichen Datensicherheitsmaßnahmen auch in diesem Fall im überwiegenden Interesse des Arbeitgebers liegt bzw. der Arbeitgeber im Regelfall datenschutzrechtlicher Verantwortlicher (Art. 4 Z 7 DSGVO) bleibt, wird angeregt, im Gesetzestext

ausdrücklich zu regeln, dass dem Arbeitnehmer auf Kosten des Arbeitgebers vorschrieben werden kann, ausreichende Datensicherheitsmaßnahmen nach Art. 32 DSGVO zu setzen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Zur Gewährleistung der Datensicherheit nach Art. 32 DSGVO könnte etwa vorgesehen werden, dass die jeweiligen Geräte regelmäßig automatische Sicherheitsupdates erhalten. Nach Möglichkeit ist die Verwendung einer geschützten WLAN- oder LAN-Verbindung und – sofern vorhanden – eine verschlüsselte VPN-Verbindung empfehlenswert. Bei der Nutzung einer offenen ungeschützten WLAN-Verbindung ist jedenfalls der Einsatz einer verschlüsselten VPN-Verbindung empfohlen. Die Endgeräte sollten insbesondere auch über eine Festplattenverschlüsselung sowie Virenprogramme verfügen.

Ergänzend wird darauf hingewiesen, dass unzureichende Datensicherheitsmaßnahmen der Sanktionsdrohung des Art. 83 Abs. 4 lit. a DSGVO unterliegt. Adressat ist der datenschutzrechtlich Verantwortliche.

Zu Artikel 3 Z 1 (§ 2 Abs. 4 DHG):

Die oben aufgeworfene Problematik ist auch im Hinblick auf § 2 Abs. 4 DHG, betreffen die Frage, wer für Schäden – die bspw. im Fall eines Hackerangriffes substantiell sein können –, die durch mangelhafte Datensicherheitsmaßnahmen verursacht wurden, haftet, relevant.

Eine Klarstellung wird angeregt.

Zu Artikel 7 Z 1 (§ 16 EStG):

Darüber hinaus erscheint unklar, ob Ausgaben, die im Zusammenhang mit Datensicherheitsmaßnahmen (Virenprogramm etc.) stehen und die ggf. vom Arbeitnehmer zu tragen sind, von den Werbungskosten gedeckt sind.

Eine Klarstellung wird angeregt.

Eine Kopie dieser Erledigung geht an das Präsidium des Nationalrates.

19. Februar 2021
Für die Leiterin der Datenschutzbehörde:
SCHMIDL