Datenschutz in Corona-Zeiten

Teil 2

Für das Arbeiten im Home-Office gelten die gleichen Datenschutz-Anforderungen wie im Büro. Neben den Kommunikationswegen (siehe: Datenschutz in Corona-Zeiten,Teil 1) gilt dies auch für die Arbeitsmittel, die hier im Mittelpunkt stehen.

Einrichtungen, die Mitarbeitende bereits mit Dienstgeräten und VPN-Zugängen entsprechend ausgestattet und geschult haben, sind natürlich besser aufgestellt als die, die durch Corona improvisieren müssen. Wer jedoch einige Vorkehrungen trifft, kann zumindest vorübergehend durchaus geschützt auch von zu Hause aus arbeiten.

Zunächst wird jedoch auf weitere Grundsätze zu Datenschutzbestimmungen und Zuständigkeiten eingegangen.

Grundsätzliches

Auf die in Teil 1 genannten Beispiele von Kommunikations-Software kamen unterschiedliche Reaktionen: Ein Träger sieht es strenger, ein anderer wegen Corona lockerer. Es mag sein, dass öffentliche Stellen auf eventuell in ihrem jeweiligen Bundesland verlautbarte Lockerungen setzen können und konfessionelle Träger auf ihre jeweiligen Aufsichtsbehörden.

Freie Träger müssen sich an den Bundesdatenschutzbeauftragten (Ulrich Kelber) halten, der Unternehmen davon abriet, „die Beschäftigten auf ihren privaten Geräten zu Hause arbeiten zu lassen. Er hoffe, dass diejenigen, die mit sensiblen Daten arbeiteten, eine angemessene Ausstattung aus der Firma bekämen – etwa einen gesicherten Laptop. Arbeitnehmern empfahl er, für jeden Dienst ein eigenes Passwort zu verwenden und wenn möglich verschiedene Geräte für Privates und Dienstliches zu verwenden“ (DLF, 29.03.2020).

Es ist also keineswegs so, dass zum Beispiel zur Aufrechterhaltung der Aufgaben quasi auf eigene Faust in das Grundrecht auf Datenschutz eingegriffen werden kann. Wie bei allen momentan verordneten Notmaßnahmen aufgrund von Corona, muss auch hier ganz genau geschaut werden, was auf welcher Rechtsgrundlage überhaupt möglich ist.

Auch Hinweise zur nötigen Konfiguration einiger Tools gingen ein. Die Texte verzichten bewusst auf die konkrete Umsetzung, denn dafür wären mehrere Seiten in IT-Sprache nötig. Letztendlich geht vermutlich vieles nur mit fachlich qualifizierten Ansprechpersonen oder gar Datenschutzbeauftragten vor Ort.

In diesem Sinn kann auch dieser Teil lediglich eine Orientierungshilfe sein.

Arbeitsgeräte

Alle für dienstliche Zwecke genutzten Endgeräte wie PCs, Laptops oder Tablets müssen auf hohem Sicherheitsstand gehalten werden. Das bedeutet, dass Updates von Firewalls, Betriebssystemen und Software aktuell aufgespielt und dass Viren-Scans durchgeführt werden. Und zwar auf privaten und dienstlichen Geräten gleichermaßen. Da das Bereitstellen entsprechender Privatgeräte durch Mitarbeitende nicht erwartet werden kann, ist deren Sicherheitsstandard immer ein Problem. Vom Einsatz privater Geräte sollte also abgesehen werden.

Wo das vorübergehend nicht anders als mit Privatgeräten geht,

- sollten keine Daten von Ratsuchenden darauf verarbeitet werden.
- müssen private und dienstliche Dateienordner, E-Mail-Eingänge usw. durch unterschiedliche Benutzerkonten getrennt werden, um die entsprechend getrennten Bereiche voreinander zu schützen.
- Die Zugangsdaten für die dienstlich genutzten Geräte und Benutzerkonten sind selbstverständlich nicht die gleichen wie für die private Nutzung.

Auf Dienstgeräten sollte keine Software installiert werden (können), die nicht mit der Einrichtung abgestimmt wurde. Wird an wichtigen Dateien gearbeitet, werden diese durch ein regelmäßiges Backup auf einer externen Festplatte oder einem USB-Stick gespeichert. Beide sollten passwortgeschützt sein, keine anderen Daten beinhalten und für Unbefugte unzugänglich aufbewahrt werden.

Zutritt und Zugang

Vor Pausen und Feierabend erfolgt immer ein Logout.

Wer mit anderen Personen im Haushalt lebt, muss auf Blickschutz für den Monitor achten, beim kurzfristigen Verlassen des Schreibtisches (der Arbeitsecke o.ä.) den Bildschirmschoner aktivieren und Papiere verstauen. Besuche und Handwerker dürften aktuell sowieso weniger üblich sein.

Den gleichen Schutz vor Zutritt durch Unbefugte wie in Büroräumen zu schaffen, wird meist schwierig sein. Trotzdem sollten Arbeitsgeräte und Arbeitspapiere in verschließbaren Schränken und Schubladen verstaut sowie Türen und Fenster (Erdgeschoss) so gut wie möglich abgeschlossen werden.

Damit Internetverbindungen vor Unbefugten geschützt sind, sollte das Gerät durch ein Kabel (LAN) mit dem Router verbunden sein. Wo das nicht geht, sollte das häusliche WLAN dem Standard WPA2 genügen und verschlüsselt angewählt werden. Was man sowieso machen sollte: Bei der ersten Inbetriebnahme das vom Hersteller mitgelieferte Gerätepasswort ändern.

Damit durch das Entsorgen von Dokumenten oder Notizzetteln im Papierkorb bzw. Hausmüll keine Datenschutzprobleme entstehen, sollten alle Papiere mit Personenbezug zunächst möglichst sicher aufbewahrt und später in der Einrichtung datenschutzgemäß entsorgt werden.

Datenpanne

Es muss geregelt sein, wer unverzüglich zu benachrichtigen ist, wenn vermutet oder festgestellt wird, dass Daten an Unbefugte gelangen oder eingesehen werden konnten, wenn eine verdächtigte Email geöffnet wurde oder wenn Geräte oder Papiere verschwunden sind.

Mehr Informationen

Bundesamt für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD):

https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Institut für e-Beratung:

https://www.e-beratungsinstitut.de/wordpress/wp-content/uploads/2020/03/IEB_1012_INFO_Onlineberatung_Corona_public.pdf

---

Anmerkungen

Alle Anforderungen an einen Arbeitsplatz im Home-Office müssen dokumentiert werden. Das geht in Corona-Zeiten vermutlich oft nur eingeschränkt, sollte aber bei eventuell nicht nur vorübergehenden Lösungen nachgeholt werden.

In diesem Text ist mit Home-Office das Arbeiten von zu Hause und nicht von unterwegs aus gemeint.

Berichtigung

In Teil 1 muss es (auf Seite 1 in der Mitte) in der Klammer hinter Post nicht Fernmeldegeheimnis, sondern Postgeheimnis heißen. Wir bitten um Entschuldigung.

In Teil 1 wurde zoom als ein Anbieter für Video-Konferenzen genannt. Inzwischen wurden Sicherheitsprobleme bekannt. Das zeigt, dass alle Nennungen immer nur tagesaktuell sein können und entsprechend überprüft werden müssen.

Verfasst von

Corinna Gekeler

Externe Datenschutzbeauftragte der bke

www.wellenlaengen-beratung.de

Herausgegeben von der

Bundeskonferenz für Erziehungsberatung e.V

www.bke.de

Stand: 02.04.2020