

Bring your own device

Bring your own device oder kurz **BYOD** ist ein Ansatz nachdem es [Beschäftigten](#) gestattet wird oder sie sogar dazu ermutigt werden, private Geräte (insb. Computer, Smartphone) dienstlich einzusetzen. Vorteile werden darin gesehen, dass die Technik den Beschäftigten vertrauter ist, so dass weniger Schulungskosten anfallen. Zudem werden auch Kosten für Anschaffung und Support dieser Geräte eingespart, wobei dem ggf. entgegensteht, dass sich Arbeitgeber an den Kosten ihrer Beschäftigten für diese Geräte beteiligen.

Im Hinblick auf den Datenschutz ist BYOD nicht unproblematisch. Eine Trennung von dienstlichen und privaten Daten wird erschwert, so dass die Beachtung der notwendigen [Trennung](#) zusätzliche [Technische und organisatorische Maßnahmen](#) nach sich zieht.

Zwangsläufig schaffen private Geräte neue, zusätzliche Angriffspunkte. Bei Smartphones gibt es sowohl zielgerichtet eingesetzte Spionage-Apps, die allerdings meist erfordern, dass ein Nutzer am Smartphone aktiv Schutzmaßnahmen durchbricht,¹⁾ als auch in offiziellen App-Shops Apps mit weitgehender Überwachung zur (angeblichen) technischen Weiterentwicklung, die durchaus auch von namhaften Anbietern stammen können.²⁾

Generelle Hinweise

Wenn BYOD nicht ausdrücklich vom Arbeitgeber zugelassen wurde, erfolgt der Einsatz durch Beschäftigte auf eigenes Risiko. (Zur Klarstellung: Eine Verpflichtung zur Nutzung von BYOD besteht nur, wenn das ausnahmsweise vereinbart wurde, zB in einer Vereinbarung zu [Tearbeit](#).) Wo BYOD ausdrücklich untersagt ist, muss das respektiert werden.³⁾

Beschäftigte sollten sorgfältig abwägen, ob sie private Technik dienstlich nutzen.

Im Regelfall ist ein Einsatz allenfalls für mobile Geräte bzw. außerhalb des dienstlichen Arbeitsplatzes sinnvoll, also im Rahmen der [Tearbeit](#). (Zu den Beschränkungen der Tearbeit an der TU Ilmenau siehe: [Tearbeit \(TU\)](#).)

Private Technik sollte nicht direkt mit dienstlicher Hardware verbunden werden, z.B. über USB, das gilt insbesondere für Speichermedien (USB-Sticks) aus unklaren Quellen (Werbegeschenke, Funde, gebraucht erworben etc.) aber auch für sonstige Technik, z.B. private Drucker, um sich den Weg zum zentralen Drucker zu sparen.

[Personenbezogene Daten](#) sollten allenfalls verarbeitet werden, wenn sie als nicht besonders sensibel (bzw. Schutzbedarf normal/mittel) eingestuft sind. Im Vergleich zu normaler [Tearbeit](#) birgt BYOD zusätzliche Risiken.

Sicherheitshinweise

Wenn private Technik zum Einsatz kommt, sollte in jedem Fall eine Mindestabsicherung entsprechend „üblicher“ Empfehlungen sichergestellt werden:

- Regelmäßige Updates
- Virens Scanner
- keine illegale Software
- keine gecrackten Softwareversionen
- kein gerootetes Betriebssystem (mobile Geräte mit Android und iOS; bei Linux nicht als Root standardmäßig arbeiten)
- Anmeldung mit nicht-trivialem Passwort (eher mindestens 12 Stellen aber merkbar)
- Browser mit sehr konsequenten Einstellungen für Privatsphäre und/oder unterschiedliche Browser für dienstliche und private Zwecke
- Einsatz qualitativ halbwegs hochwertiger Technik - keine Billigware oder gar Werbegeschenke

Ergänzend sollten die Sicherheitshinweise im Artikel [Tearbeit](#) beachtet werden.

Weblinks

- [Der Bayerische Landesbeauftragte für den Datenschutz \(BayLfD\): Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie, Seite bei archive.org.](#)
- [Conrad in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Rn. 293-301, 2. Auflage 2016](#)
- [Hoppe in Kramer, IT-Arbeitsrecht, Rn. 616-618, Rn. 727-634, 1. Auflage 2017](#)

Artikel

¹⁾

Vgl. [heise.de:Alptraum Handy-Wanzen: Wie Nutzer per Smartphone überwacht werden können.](#)

²⁾

Vgl. [heise.de:Bericht: Populäre Apps zeichnen heimlich iPhone-Bildschirm auf.](#)

³⁾

Gemäß [Art. 4](#) Nr. 7 DSGVO legt der [Verantwortliche](#) die Mittel der Verarbeitung fest, wozu auch die eingesetzte Hard- und Software gehört. Der Verantwortliche für eine Verarbeitung ist in der Arbeitgeber-Arbeitnehmer Konstellation aber in aller Regel der - weisungsberechtigte - Arbeitgeber.

From:

<https://141.24.186.195/> - **DS-Wiki**

Permanent link:

https://141.24.186.195/bring_your_own_device

Last update: **2022/02/25 11:16**

