

Ubiquitous Computing – Erste Hilfe

In einer Welt alltagsgegenwärtiger Datenverarbeitung ("ubiquitous computing") haben Sie nur wenige Chancen, den Folgen intensiver Datenerfassung und deren vernetzter Auswertung zu entgehen. Aber die sollten Sie unbedingt nutzen.

Am Arbeitsplatz dürfte Ihre Hilflosigkeit am größten sein: Was immer Ihr Arbeitgeber oder Dienstherr an rechnergestützten Techniken plant – Sie haben gerade in heutiger Zeit Sorge um Ihren Job und nehmen es hin. Ist doch so, oder? Nicht ganz: Sie haben grundlegende Rechte, die können Sie, wie bereits erwähnt, mit entsprechender Hilfe auch nutzen ohne Nachteile zu riskieren. Ihre Helfer können wache betriebliche Datenschutzbeauftragte sein oder engagierte Betriebsräte – oder Sie können sich jederzeit an uns als Datenschutzbehörde wenden, wir beraten Sie gerne. Mehr noch: Wenn wir Ihre Sorgen und Bedenken nicht im Gespräch zerstreuen können, sondern die Notwendigkeit sehen, in Ihrem Betrieb tätig zu werden, wahren wir auf Wunsch Ihre Anonymität.

In Ihrem privaten Umfeld haben Sie hingegen weitaus mehr Möglichkeiten, sich und Ihre Privatsphäre zu schützen. Sie müssen es nur wollen – manchmal bedeutet Datenschutz eben auch Verzicht auf vermeintliche Bequemlichkeit. Wann immer Sie über den Erwerb oder die Anmietung rechnergestützter Anwendungen in Ihrem persönlichen Alltag nachdenken, sollten Sie jeweils den Nutzen der eingesetzten beziehungsweise einzusetzenden Technologie abwägen gegen die möglichen Gefahren einer unkontrollierbaren Datenpreisgabe. Achten Sie darauf, dass in derartige Geräte möglichst keine Funktionen eingebaut sind, die eine alltagsgegenwärtige Datenverarbeitung erfordern oder gar voraussetzen.

Falls sich das aber nicht vermeiden lässt, sollten Sie derartige Funktionen auf ein Minimum beschränken. Wenn Sie es etwa mit Anwendungen zu tun haben, die an transportable Systeme wie mit RFID-Chips ausgestattete Chipkarten geknüpft sind, sollten Sie Schutzhüllen aus metallischen Materialien (zum Beispiel Alufolie) verwenden, das behindert – oder verhindert, je nach Leistung – die ungewollte Übermittlung von Daten. Sie sollten verschiedene Systeme möglichst nicht miteinander verbinden, weder per Kabel noch mittels Funkschnittstellen wie Bluetooth, wenn dies nicht unbedingt notwendig ist: Ob Sie entsprechende Funktionen erst gar nicht aktivieren oder ob Sie in Geräten mit werksseitig aktivierten Funktionen diese außer Betrieb setzen, ist dabei egal: Unterbinden Sie unkontrollierten Datenaustausch Und selbst dort, wo Sie keine unmittelbare Vernetzung sehen oder ahnen, kann Vorsicht geboten sein, auch eine gemeinsame – oder zeitgleiche – Nutzung unterschiedlicher Systeme kann ein Risiko für Ihre Privatheit bedeuten. Wenn Sie an der Discounterkasse erst Ihre Kundenkarte zücken, um dann mit

Ihrer EC-Karte zu bezahlen, schaffen Sie die Voraussetzung, Ihre Kunden- mit Ihren Kontodaten zu verknüpfen: Tschüs, Privatsphäre!