LEGAL DATA

DATENSCHUTZ EINFACH UND SICHER UMSETZEN

CHECKLISTE HOME OFFICE UND

WWW.LEGALDATA.LAW

CHECKLISTE -DATENSCHUTZ IM HOME OFFICE

Gesicherte Systemumgebung/ Technische Anforderungen

Nutzen Sie ausschließlich **die gesicherte Systemumg** Ihres Unternehmens. Die Anforderungen richten sich technisch nach dem IT Grundschutz Kompendium: Wichtig ist vor allem ein gesicherter **VPN** Zugang zum Firmennetzwerk und eine **verschlüsselte Festplatte**. Weiterhin gehört eine **Zwei-Faktor Authentifizierzung** zum gesetzlichen Standard. Eine vollständoige Übersicht zu allen technischen Anforderungen finden Sie am Ende dieser Checkliste.

WLAN Sichern

Im Home-Office wird das Heimnetzwerk zuim Firmennetzwerk. Bei einem Angriff über das WLAN sind aber nun auch sensible Firmendaten betroffen. Praxistipp: Das **WLAN Standard-Passwort** sollte unbedingt geändert werden, da es ansonsten sehr einfach ist, auf Ihr Netzwerk zuzugreifen.

„Schatz2002“ - Sichere Passwörter verwenden

Einfache Passwörter stellen ein hohes und inder Praxis unterschätztes Risiko dar: Mit s.g. Bruteforce-Attacken können einfache Passwörter sehr schnell und einfach gehackt werden. Der Angreifer hat dann sehr einfach Zugriff auf vertrauliche Daten. Wer sich davor schützen will, muss lange, zufällige und einzigartige Kennwörter verwenden. Sonderzeichen sind aus Praxissicht eher weniger relavent. **Entscheidend ist aber die Länge:** Zwölf Zeichen sind das Minimum, für wichtige Konten empfehlen sich mindestens 16 Buchstaben und Ziffern. Viele Nutzer verwenden dasselbe Kennwort für mehrere Konten oder variieren es nur geringfügig. Das ist eine Einladung an Hacker. Deshalb sollte man einen Passwort-Manager wie 1Password, LastPass oder die Open-Source-Lösung KeePass nutzen. Diese Programme generieren zufällige und sichere

Kennwörter und speichern sie verschlüsselt ab.

Dropbox & Co. – Daten sicher abspeichern

Firmendokumente gehören **nicht** in eine Cloud wie Dropbox oder OneDrive. Sie sollten ausschließlich auf dem Firmennetzwerk gespeichert werden. Falls unbeidngt erforderlich, sollte man lokalen Dateien mit einer Software wie Veracrypt verschlüsseln. Windows (BitLocker) und MacOS (FileVault) bieten dafür auch integrierte Lösungen an.

Trennung - auch bei den Daten und Müll!

Viele Menschen nutzen aktuell **ein Gerät** für alles. Das sollte unbedingt vermieden werden, denn ein privates Gerät hat oft einen wesentlich geringeren Schutz als ein Firmenlaptopb (welches den BSI Anforderungen unzterlichen sollte – siehe die Links hierzu unten). Ein hohes Risiko stellen auch Weiterleitungen von Dokumenten per E-Mail auf einen privaten E-Mail Account dar. Ausdrucke von Firmenunterlagen gehören auf keinen Fall in den Hausmüll und sollten geschreddert werden. Günstige Schredder sind auch für das Home-Offce erschwinglich.

„I love you#“ Mitdenken – Nur bekannte Anhänge öffnen

Der größte Risikofaktor ist der **User** selbt. Die sicherste Hardware hilft nichts, wenn Nutzer leichtfertig Anhänge öffnen, Dateien herunterladen und Programme installieren. Wer einem Absender oder Entwickler nicht zu 100 Prozent vertraut, sollte die Finger davon lassen. Im Home-Office ist es schwieriger, schnell Kollegen um Rat zu fragen, und die IT-Abteilungen sind oft überlastet. Trotzdem kann ein kurzer Anruf oder eine Google Recherche viel Ärger ersparen.

Technische Details

Alle technischen Details für eine korrekte technische Umsetzung der gesetzlichen Anforderungen finden Sie unter den nachfolgenden Links:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_4_Telearbeit.html

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_9_Mobiler_Arbeitsplatz.html

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_8_H%C3%A4uslicher_Arbeitsplatz.html

ÜBER UNS

“Datenschutz soll nicht daran hindern, Ihr Geschäft voranzubringen.Im Gegenteil: Eine professionelle Lösung des Themas wird immer wichtiger - auch gegenüber Kunden und Geschäftspartnern.“

Datenschutz. Einfach und sicher umsetzen.

Unter diesem Motto steht unserem Team mit legal data, ab dem 01.04.2020 eine moderne und zeitgemäße Plattform zur Verfügung, mit der wir unsere langjährigen Mandanten in das nächste Jahrzehnt begleiten werden.

Hochsichere Systeme, eine auf unsere Bedürfnisse abgestimmte DMS-Software, eine 24/7 Datenschutzhotline für Datenschutzverstöße und Notfälle sowie eine eigene Schulungsplattform stellen eine moderne und professionelle Betreuung sicher.

HISTORIE

Im Mittelpunkt steht aber seit mehr als zwanzig Jahren der Mandant: Im Datenschutzrecht und als Datenschutzbeauftragter ist es unsere erste Aufgabe, die Compliance mit allen datenschutzrechtlichen Vorschriften sicherzustellen und Bußgelder von Ihrem Unternehmen fernzuhalten.

PRAGMATISCHE LÖSUNGEN

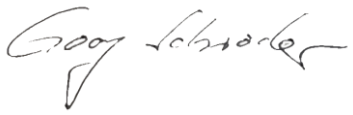
Dabei schaffen wir aber auch pragmatische und einfache Lösungen. Denn der Datenschutz im Unternehmen soll Sie nicht hindern, Ihr Geschäft voranzubringen, sondern ein Aushängeschild für Ihre Mitarbeiter und Kunden in einem modernen Unternehmen sein.

Sicherheit.
Dafür stehen wir.

SICHERHEIT

Als in Deutschland zugelassene Rechtsanwaltsgesellschaft haften unsere Anwälte und Datenschutzbeauftragte persönlich. Mit unserem auf die neuen Bußgeldrisiken der DS-GVO konzipierten Versicherungskonzept, welches Schäden von bis zu 40 Millionen EURO abdeckt, schaffen wir für Sie und uns Sicherheit. In einer digitalen Welt.

Hierfür stehe ich mit meinem Wort.
Ihr



Dr. Georg F. Schröder, LL.M.
Geschäftsführer
Rechtsanwalt
Datenschutzbeauftragter

Dafür stehen wir:

- Mehr als 20 Jahre Erfahrung im Datenschutzrecht
- Versicherungsschutz mit 40 Mio. Deckungssumme
- Compliance im Datenschutz und pragmatische Lösungen

KONTAKT

legal data
Schröder
Rechtsanwaltsgesellschaft mbH
Prannerstr. 10
80333 München

Tel:
+49 89 954 597
520
Fax:
+49 89 954 597 522

E-mail:
datenschutz@legaldata.law
www.legaldata.law