**Datenschutz – Deutsche Richtlinien**

Das deutsche **Bundesdatenschutzgesetz** (**BDSG**) regelt zusammen mit den Datenschutzgesetzen der [Länder](http://de.wikipedia.org/wiki/Land_%28Deutschland%29) und anderen bereichsspezifischen Regelungen den Umgang mit [personenbezogenen Daten](http://de.wikipedia.org/wiki/Personenbezogene_Daten), die in [Informations- und Kommunikationssystemen](http://de.wikipedia.org/wiki/Information_und_Kommunikation) oder manuell verarbeitet werden.

**Überblick über das BDSG**

Das BDSG besteht aus sechs Abschnitten:

* Im ersten Abschnitt (§§ 1–11) werden allgemeine und gemeinsame Bestimmungen erläutert,
* im zweiten Abschnitt (§§ 12–26) die Datenverarbeitung für öffentliche Stellen und
* im dritten Abschnitt (§§ 27–38a) für private Stellen geregelt.
* Der vierte Abschnitt (§§ 39–42) enthält Sondervorschriften,
* im fünften Abschnitt (§§ 43–44) werden Straf- und Bußgeldvorschriften und
* im sechsten Abschnitt (§§ 45–46) Übergangsvorschriften genannt.



**Wie schütze ich meine Daten am besten?**

1) ALLES kritisch hinterfragen  
Reicht nicht eigentlich nur die Angabe meiner E-Mail-Adresse, um Kontakt zu mir aufzunehmen? Warum soll ich auch noch Adresse und Telefonnummer angeben?   
Anbieter versuchen so viele Informationen wie möglich von Internet-Nutzern zu bekommen, um diese dann weiterzuverkaufen.

2) Kann ich meinen Computer sicherer machen?  
Jeder Computer, der zum Surfen im Internet und für Bankgeschäfte verwendet wird, sollte über einen Virenscanner und eine Firewall verfügen. Beide sollten überdies regelmäßig aktualisiert werden.  
3) Daten auf Festplatten verschlüsseln  
Empfehlenswert ist auch die Verschlüsselung wichtiger Daten und Dokumente auf Deiner Festplatte oder, sofern Du diese nutzt, auch in Cloud-Diensten. Ein Programm für die Verschlüsselung ist [TrueCrypt](http://www.truecrypt.org/). Für Nutzer von Cloud-Diensten, die ihre Daten verschlüsselt auch Dritten zur Verfügung stellen wollen, gibt es weitere Programme wie [BoxCryptor](http://www.boxcryptor.com/?lang=de) oder [Safebox](http://www.safeboxapp.com/welcome.html).

4) Wie kann ich meine IP-Adresse verschleiern?   
Eine Möglichkeit, die eigene Herkunft – also die eigene IP-Adresse – zu verschleiern, ist die Nutzung eines Virtual Private Networks (VPN).   
Dabei wird neben der Internetverbindung mit Deinem Internetanbieter eine weitere direkte Verbindung zu einem anderen Server aufgebaut, über den dann jeglicher Datenverkehr geleitet wird. Jemand Drittes kann Dein Surfverhalten so nicht mehr analysieren.

* kostenlose Angebote von einigen Universitäten und andere teils nur zeitweise verfügbare VPN-Server.
* Internetverbindung deutlich langsamer ist.
* Aber: Der Schutz ist nur begrenzt, da der VPN-Server selbst oftmals alle Daten von Dir hat, sofern er diese speichert.

5) Wie kann ich meine Kontodaten gegen Betrüger schützen?  
Niemals auf Spam-Mails antworten → ungelesen löschen  
E-Mails enthalten Viren oder Programme zum Ausspähen des Computers.   
Vorsicht außerdem vor gefälschten E-Mails, die versuchen Passwörter und Bankverbindung des Nutzers abzufragen. Keine Bank würde diese Daten per E-Mail abfragen, es kann sich also nur um Betrüger handeln.

6) Wo lauern außerdem Gefahren?  
Soziale Netzwerke wie Facebook, StudiVZ und ähnliche sammeln eine Unmenge sehr persönlicher Daten über jedes Mitglied. Ihr Geschäftsmodell basiert darauf, diese Daten für Werbekunden aufzubereiten. Dagegen können Mitglieder sich auch nicht durch strenge Filtereinstellungen schützen.→ So wenig wie möglich privates Preisgeben! Kein Geburtstag, Wohnort/Adresse, Ortungen

7) Wie oft sollte ich meine Passwörter ändern?  
Passwörter schützen auf Computern und im Internet E-Mails, das Bankkonto und noch sehr viel mehr.   
- drei bis vier Monate ändern  
- Austauschen oder Umdrehen von Buchstaben oder Zahlen  
- Regelmäßig sollten Ihre Passwörter aber auch komplett geändert werden

8) Anonym suchen- Alternative zu Google  
Google ist die meist verwendete Suchmaschine. Über die Suche verrät man sehr viel über die Interessen und Vorlieben. Insbesondere wenn man bei Google parallel andere Dienste nutzt und während der Suche eingeloggt ist.  
Auch ohne Einloggen ist Bildung weitreichender Profile möglich.   
Anbieter, die sich explizit den Schutz Deiner Daten und Deiner Privatsphäre auf die Fahnen geschrieben haben – zum Beispiel [ixquick.com](https://www.ixquick.com/deu/).

9) Inhalte verschlüsseln   
E-Mails sind im Prinzip nicht sicherer als Postkarten. Da die Inhalte digital sind, ist eine automatisierte Auswertung dieser, zum Beispiel durch eine Rasterung nach bestimmten Suchworten, sehr einfach. Die Inhalte von Mails lassen sich jedoch relativ einfach verschlüsseln. Die beiden am meisten verwendeten Computerprogramme für asymmetrische Verschlüsselung sind [Pretty Good Privacy (PGP)](http://www.openpgp.org/) and [GNU Privacy Guard (GnuPG)](http://www.gnupg.org/). Die Benutzung dieser Programme ist der beste Weg, Deine E-Mails und ihren Inhalt sicherzustellen.