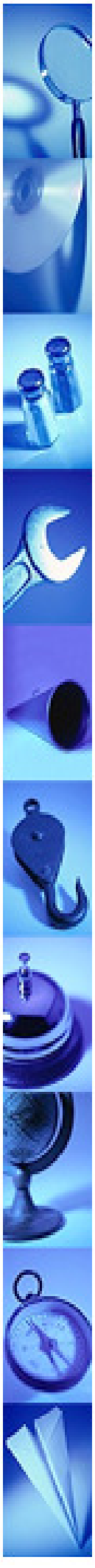


SKYNET IT

www.skynet-it.de

Checkliste zur Daten- und IT-Sicherheit nach der Änderung des Bundesdatenschutzgesetzes vom 03.07.2009

Mit Neufassung vom Juli 2009 wurden u.a. folgende Bereiche des Bundesdatenschutzgesetzes (BDSG) angepasst:

Bußgelder:
Kleinere Ordnungswidrigkeiten können mit einer Geldbuße von bis zu EUR 50.000,00 geahndet und schwerwiegende Vergehen mit bis zu EUR 300.000,00 bestraft werden. Vorher handelte es sich um EUR 25.000,00 bzw. EUR 250.000,00.

Hierbei kommt die sog. Durchgriffshaftung zur Anwendung, d.h. sogar Verantwortliche von juristischen Personen haften mit Ihrem Privatvermögen. Haftungen i.R.d. folgenden Gesetze bleiben davon unberührt und können weitere Schadensersatzansprüche nach sich ziehen:

- Postgeheimnis § 206 StGB
- Verschwiegenheitspflicht § 203 StGB
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG)
- Aktiengesetz (AktG)
- Steuerberatungsgesetz (StBerG)
- Wirtschaftsprüferordnung (WiPrO)

Datenschutzbeauftragte:
Bei elektronischer Verarbeitung bestimmter sensibler / personenbezogener Daten ist ein Datenschutzbeauftragter schon unter 10 Mitarbeitern Pflicht .

Die Neuregelung des BDSG bestimmt, dass Firmen, auch wenn Sie nur aus einer Person bestehen (Steuerberater, Ärzte, Hoteliers, Handelsvertreter, etc) einen Datenschutzbeauftragten bestellen müssen, wenn personenbezogene Daten elektronisch verarbeitet werden.

Speicherung und Vorhaltung von Verbindungsdaten:
Das Bundeskriminalamtsgesetz (BKAG) verlangt eine Datenvorhaltung für Verbindungsdaten für eine Dauer von mindestens 6 Monaten.

Betroffen hiervon sind natürlich in erster Linie alle Internet- bzw. Mailprovider, sowie Betreiber offener W-LANS (Hotels, Gaststätten, Flughäfen, Vereine ,etc.) Sollten Sie Ihren Mitarbeitern jedoch gestatten, private Mails am Arbeitsplatz zu empfangen, treten Sie automatisch als Provider für Ihre Angestellten auf und werden von den Strafverfolgungsbehörden entsprechend behandelt.

Datenschutzrechtliche Fragestellungen im Allgemeinen:

Verbreitung und Zugang zu illegalen Daten:
Hierunter fallen z.B. der Besitz oder die Verbreitung kinderpornografischer oder rassistischer Inhalte. Ein solches Vergehen wird nach dem § 184b StGB, sowie dem Jugendschutzgesetz unter empfindliche Strafen gestellt.

Die innerdeutsche Meinung verteufelt ein Delikt nach § 184b StGB aufs äußerste und erklärt, dass die Strafen für ein solches Verhalten nicht hoch genug sein können. **Aber:** Können Sie sich sicher sein, dass bedingt durch einen Trojaner, evtl. auch durch interne Mitarbeiter oder durch einen fehlerhaft konfigurierten Mailserver (offenes Relay), Ihr System Spammails mit genau diesen Inhalten verbreitet? Die dadurch im Internet hinterlassenen Spuren können nicht mehr beseitigt werden.

Verstöße gegen das Urheberrecht:
Schadensersatzforderungen für Verbreitung und Bereitstellung illegaler Raubkopien (Musik, Filme, Software, Bilder) im Internet.

Ein solcher Verstoß kann teure Folgen haben. Können Sie die Hand für Ihre Auszubildenden oder Angestellten ins Feuer legen, dass diese keine Software, Musik, etc. aus dem Internet laden. Sie haften in jedem Falle für erhebliche Forderungen.

Pflichtangaben in betrieblichen Mailings:
Zum 01.01.2007 trat das das "Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister" (EHUG) in Kraft.

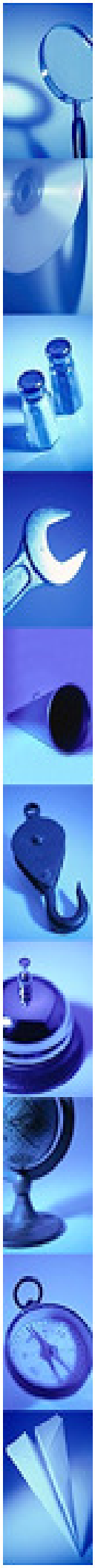
Bezogen auf diese Regelung müssen dadurch in betrieblichen Mails folgende Mindestinformationen gegeben sein.

- Firmenname
- Firmensitz
- Registergericht: Amtsgericht
- Registergericht: HRA Nummer

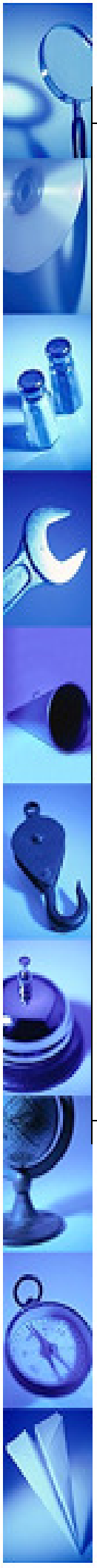
Sie haften auch dann wenn:

- Kein Mitwissen Ihrerseits vorliegt
- Ihre Mitarbeiter fahrlässig handeln
- Dritte Ihre Systeme ohne Ihre Zustimmung, evtl. durch Trojaner oder Bots benutzen
- Sie Ihrer Nachweispflicht nicht nachgekommen sind
- Sie keinen verantwortlichen Datenschutzbeauftragten schriftlich bestimmt haben
- Und Sie keine geeigneten technischen Maßnahmen veranlaßt haben.

Strategische Sicherheit	Antwort: Ja	nein	Notizen:
Gibt es im Unternehmen eine Dokumentation über IT Sicherheitskonzepte ? Pläne über Sicherheitsziele sollten darin abgebildet und definiert sein und die Umsetzung der Sicherheitsziele sollte darin geregelt sein.	☐	☐	
Wurde ein Handlungsplan erstellt, der zum Ein- und Austritt von Mitarbeitern abgearbeitet wird ? Darin enthaltene Anweisungen geben Aufschluß über die Behandlung von systemweiten Berechtigungen, Schlüssel, Passwörter und genutzte Programme.	☐	☐	
Gibt es im Unternehmen einen qualifizierten Mitarbeiter, der sich um Aspekte der IT Sicherheit kümmert ?	☐	☐	
Gibt es im Unternehmen einen schriftlich ernannten, qualifizierten Datenschutzbeauftragten ?	☐	☐	
Wurden im Unternehmen Notfallpläne / Checklisten erstellt, die abgearbeitet werden können, wenn die EDV ausfällt ?	☐	☐	
Werden Sicherheitskonzepte, Handlungs- und Notfallpläne regelmäßig überprüft ?	☐	☐	
Können im Unternehmen Daten über Netzwerkverkehr überwacht, protokolliert, gefiltert und archiviert werden?	☐	☐	
Werden Datenträger, die sensitive Daten speichern gesondert und sorgfältig aufbewahrt?	☐	☐	
Werden sensitive Daten vor fälligen Wartungs- und Reparaturarbeiten rückstandslos von Datenträgern entfernt?	☐	☐	
Werden die für die IT Sicherheit verantwortlichen Mitarbeiter regelmäßig, speziell geschult?	☐	☐	
Werden im Unternehmen spezielle IT Sicherheits-Produkte eingesetzt und regelmäßig auf den aktuellen technischen Stand gebracht?	☐	☐	



Operative Sicherheit	Antwort: Ja	nein	Notizen:
Datensicherung:			
Wird eine netzwerkweite Datensicherung auf Bandlaufwerk durchgeführt?	☐	☐	
Wurde im Unternehmen eine Backup Strategie schriftlich festgehalten?	☐	☐	
Benutzen Sie externe USB Geräte zur Datensicherung?	☐	☐	
Sind Datensicherungsgeräte vor Überspannungs-, Feuer-, Wasser und Überhitzungsschäden gesichert?	☐	☐	
Gibt es Richtlinien zum Umgang und Lagerung von Backupmedien.	☐	☐	
Infrastruktur:			
Besteht ein ausreichender Schutz der Infrastruktur gegen Überspannungs-, Feuer-, Wasser- und Überhitzungsschäden?	☐	☐	
Gibt es einen geregelten Zutrittsschutz zu Schlüsselsystemen und –räumen?			
Werden Handwerker / Servicekräfte in IT Räumen begleitet bzw. beaufsichtigt?	☐	☐	
Wurde die Leistung/Funktionalität von Netzwerkkabeln dokumentiert / zertifiziert?	☐	☐	
Gibt es im Unternehmen eine Dokumentation über Infrastrukturgeräte, Hard- und Software?	☐	☐	
Wird das Patchen von Netzwerkdosen sofort dokumentiert?	☐	☐	
Dokumentationen:			
Gibt es im Unternehmen eine Dokumentation über die wichtigsten Passwörter, Zugangsdaten zu Providern, Berechtigungsstrukturen und Infrastrukturkomponenten, die im Notfall herangezogen werden können?	☐	☐	
Gibt es Pläne und Kontaktadressen, die im Notfall jedem Mitarbeiter zugänglich sind?	☐	☐	
Kennt jeder Mitarbeiter den Notfallplan und den Zugang zu den wichtigsten Kontaktadressen?	☐	☐	
Passwort- und Berechtigungsstruktur:			
Hat jeder Benutzer ein eigenes Profil, abgesichert durch ein sicheres Kennwort?	☐	☐	
Sind die Benutzer im Umgang und der Erstellung sicherer Passwörter geschult?	☐	☐	
Gibt es im Unternehmen eine Berechtigungsstruktur, die regelt welche Benutzer auf welche Daten zugreifen können?	☐	☐	
Ist diese Berechtigunsstruktur dokumentiert?	☐	☐	



Operative Sicherheit	Antwort: Ja	nein	Notizen:
Systemupdates: Werden im Unternehmen regelmäßig die aktuellen Hard- und Softwareupdates eingespielt?	☐	☐	
Werden diese Updates vor systemweiter Einspielung umfassend getestet?	☐	☐	
Gibt es hierfür eine Testumgebung?	☐	☐	
Wurde im Unternehmen ein Verantwortlicher bestimmt, der den Umgang mit Sicherheitsupdates überwacht?	☐	☐	
Allgemeines: Gibt es auf den unternehmensweiten Systemen Sicherheitsmechanismen, wie z.B. Festplattenverschlüsselungssoftware?	☐	☐	
Werden insbesondere mobile Systeme wie Notebooks und deren Backupsysteme entsprechend verschlüsselt?	☐	☐	
Sperren Mitarbeiter beim Verlassen der Rechner Ihre Desktops mit Bildschirmschoner und Kennworteingabe?	☐	☐	
Sind Kunden-, Patienten- oder Mandantenakten von externen Personen einsehbar?	☐	☐	
Gibt es im Unternehmen eine W- / D- LAN Verbindung?	☐	☐	
Versenden Sie im Newsletter / Infomails an Ihre Kunden?	☐	☐	
Sind im Unternehmen ungenutzte Netzwerkdosen aktiv / gepatcht?	☐	☐	
Ist es im Unternehmen gestattet private Mails am Arbeitsplatz zu senden / empfangen?	☐	☐	

Bitte senden Sie die Checkliste zur Auswertung per Mail oder Fax an die SkyNet *IT* GmbH, wir werden uns diesbezüglich schnellstmöglich bei Ihnen melden. Sollten Sie bei der Bearbeitung der Checkliste Fragen- oder Probleme haben, so stehen wir Ihnen unter folgenden Rufnummern gerne zur Verfügung.

SkyNet-*IT* GmbH

Ludwig-Zorn-Straße 4

D - 75031 Eppingen

Tel.: +49 7262 91 27 18

Fax.: +49 7262 91 27 17

Hotline.: +49 171 80 28 426

http://www.skynet-it.de

info@skynet-it.de