







Informationen für Diplom-Psychologinnen und -Psychologen zur Informations-Technologie und zur beruflichen Telekommunikation (Version September 2008)





(A) Telefon-Datenschutz

- ☎ Die **Anrufer-Nummernanzeige** möge zur Gewährleistung der Anrufer-Anonymität – zumindest in Beratungs-Einrichtungen für hochsensible Themen – unterdrückt werden. T-Com-Leistung „CLIP“; dies wird im Telefonbuch angezeigt.
- ☎ Bei abgehenden Telefonaten die **Rufnummern-Übertragung** der Einrichtung zum angerufenen Anschluss abstellen (T-Com-Leistung „CLIR“; „Rufnummern-Unterdrückung“), um die dortige Anzeige zu verhindern – ansonsten nur mit vorheriger Einverständnis-Einholung.
- ☎ Ggf. die **Inverssuche** (Namenssuche von der Rufnummer ausgehend) für elektronische Telefon-Verzeichnisse untersagen.
- ☎ Verzicht auf die **Einzelverbindungsübersicht**, den Einzelverbindungs nachweis bei der Telefon-Rechnung mit zu schützenden Klienten-Rufnummern.
- ☎ Verzicht auf die **Verbindungsdaten-Speicherung in Einrichtungen**, deren Kontakte wegen des Privatgeheimnisschutzes gemäß § 203 StGB nicht anderweitig bekannt werden dürfen – z. B. ist eine „Abrechnungsstelle“ der Verwaltung nicht „Gehilfe“ im Sinne des StGB.
- ☎ Wegen der **Vorratsdatenspeicherung** (VDS) mit Kliententelefonaten allgemein zurückhaltend bleiben, ggf. auch nur mit vorheriger Einverständnis-Einholung. (Wegen der Vorratsdatenspeicherung (VDS) ist mit vermehrt persönlicher Kontaktaufnahme durch Ratsuchende zu rechnen, die die VDS vermeiden wollen. Die VDS speichert auch die Orte von Handytelefonaten.)

-  Mithörgelegenheiten durch Unbefugte sind zu verhindern, z. B. im Wartezimmer, bei der Anmeldung, in der Sprechstunde. „Laut Mithören“ (Telefon-Lautsprecher) ist dem Gesprächspartner mitzuteilen, die weiteren Zuhörenden sind zu nennen.
-  Faxzusendung sollte mit sichergestellt „geschütztem“ Empfang beim Adressaten erfolgen. Faxgeräte sind außerhalb von Einsichts-Möglichkeiten durch Unbefugte aufzustellen.
-  Bei Rufnummern-Listen im Festnetztelefon und im Handy auf deren Speicherungen verzichten, z. B. „Telefonbuch“, eingegangene, abgegangene, versuchte Verbindungen.
-  Beim Telefonieren über VoIP (Voice over Internet Protocol, „Internet-Telefonie“) besteht ohne Verschlüsselung kein Mithörschutz!

(B) Berufliche PC-Nutzung

(PC und/oder Notebook/Laptop/Handheld u. ä.; ohne Internetverbindung¹)

-  Der **Zugang zu allen Geräten** ist (für den Datenschutz und den Privatgeheimnisschutz) sorgfältig zu regeln, der Dateien-Zugang und die Einsicht durch Unberechtigte sind zu verhindern. „Besondere Arten personenbezogener Daten“ sind im Bundesdatenschutzgesetz (BDSG) § 3, Abs. 9 ausdrücklich geregelt.
-  **Passwörter** (verschiedene, lange und ausreichend komplizierte aus Klein-/Groß-Buchstaben, Ziffern und Zeichen) einführen, regelmäßig ändern und versteckt aufbewahren: Fürs gesamte PC-Einschalten/-Hochfahren, nach Bildschirm-schoner-Aktivierung, für das Aufrufen der Einzeldateien – und auch bei E-Mail- und Internet-Betrieb.
-  Wegen der erhöhten Diebstahl- und **Verlust-Gefahr bei Notebooks** sind das Einschalten/Hochfahren mit einer PIN zu schützen und alle einzelnen Daten **verschlüsselt** zu speichern.
-  **Datensicherung** (gegen Datenverlust) regelmäßig ausführen, besonders für selbst erstellte, selbst bearbeitete Dateien usw.; die Sicherungs-CDs, -DVDs, -USB-Sticks usw. sind verschlossen aufzubewahren. Vollständige Datenträger-

¹ Getrennte Systeme – ein PC/Notebook ohne und ein PC/Notebook mit Internet-Verbindung – sind prinzipiell für den Datenschutz zu bevorzugen. Nachteilig sind höhere Kosten und gelegentliche Umständlichkeiten beim Dateien-Einzeltransport zwischen den Systemen.

Löschung sicherstellen – auch vor USB-Stick-, PC-, Festplatten-Verkauf oder -Weitergabe.

- 🖥️ **Datenlöschung** einfach versus vollständig: Einfache Löschung bewirkt nur das Verschwinden aus den sichtbaren Verzeichnissen (inkl. „Papierkorb“). Erst vollständige Löschung mit einer zusätzlichen Software verhindert durch Überschreiben die Wiederherstellungsmöglichkeit auf der Festplatte, dem USB-Stick usw.
- 🖥️ Dauer der Daten-Aufbewahrung sowie deren vollständige Löschung – durch Überschreiben z. B. gemäß DIN 55 858 (04/1993) – und die Datenträger-Vernichtung systematisch regeln und ggf. durchführen.
- 🖥️ Regelungen der Daten-Aufbewahrung, der definierten Weitergabe sowie deren vollständiger Löschung für Fälle von Mitarbeiter- oder Praxis-Mitglieder-Wechsel frühzeitig klären. (Der Privatgeheimnisschutz ist personengebunden.)
- 🖥️ Vor **Beanspruchung von PC-Diensten** (z. B. für Service und Wartung) sind die Klientendaten sowohl zu sichern als auch von der Festplatte vollständig zu entfernen. Oder die Dienstleister sind als „Gehilfen“ des Berufspsychologen gemäß § 203 StGB (Privatgeheimnisschutz) zu verpflichten bzw. ist deren Tätigkeit zu beaufsichtigen. Eingesetzte Backup-Festplatten z. B. sind unter Kontrolle zu halten. Ggf. ist auch zu ermitteln, für welche Firmen usw. der PC-Dienst ansonsten tätig ist (wegen formloser Vertraulichkeitszusagen und der Begehrlichkeiten).
- 🖥️ **Probelaufe für neue Software** und Anwendungstests dürfen ausschließlich mit fiktiven Daten erfolgen. Die Echtdaten-Verwendung mit „besonderen Arten personenbezogener Daten“ ist im Bundesdatenschutzgesetz (BDSG) ausdrücklich untersagt.
- 🖥️ Mit eigenen Informations-Technologie-Kenntnissen sollte eine **Sicherheitskultur** und Sicherheits-Bewusstsein mit Alltags-Gewohnheiten und Engagement entwickelt werden, auch unter Rechts-, Haftungs- und Verantwortungs-Gesichtspunkten.
- 🖥️ **Mitarbeiter-Sensibilisierung und -Aufmerksamkeit** ist durch die Leitung mit Beteiligung aller wiederholt und ausführlich erforderlich. Zuständigkeiten und Verantwortungen sind klar zuregeln. Das betrifft auch die Regelung der privaten Nutzung am Arbeitsplatz.

- 🖨 Ein **Betrieblicher Datenschutzbeauftragte/r** ist gemäß § 4f BDSG in Einrichtungen mit mehr als neun Personen zu bestellen, die mit personenbezogenen Daten arbeiten.








(C) E-Mail-Verkehr

- 📧 **Berufliche E-Mail-Nutzung** erfordert wegen des Privatgeheimnisschutzes ausnahmslos die **Verschlüsselung des E-Mail-Textes und der Anlagen**. Zur E-Mail-Verschlüsselung wird eine Software für den Betrieb mit der E-Mail-Software und eine weitere Software für das Verschlüsseln benötigt. Andernfalls ist auf die einfache E-Mail-Nutzung – Absenden und Empfangen – zu verzichten in Einrichtungen und Praxen mit privatgeheimnisgeschützten Tätigkeiten (§ 203 StGB).
- 📧 Datenübermittlung grundsätzlich nur ebenso vorsichtig und geprüft wie mit post-schriftlichen Weitergaben – bezüglich Herausgabeberechtigung, genauem Adressaten. Auf **Disclaimer** („Falsch-Abgesendet-oder-Falsch-Zugesendet-Rettungsversuch-Anmerkungen“) kann verzichtet werden. Die Verantwortung der Übermittlung liegt allein beim Absendenden. Der Eindruck gewohnheitsmäßig mangelnder Sorgfalt möge vermieden werden.
- 📧 **Absenderangabe („Signatur“)** für die E-Mails einrichten, immer eine gleiche oder z. B. wahlweise für private oder berufliche Nutzung – dabei die Vollständigkeits-Erfordernisse berücksichtigen bzgl. der „Pflichtangaben“ (lediglich orientiert am Gesetz über Elektronische Handelsregister sowie das Unternehmensregister, EHUG).
- 📧 Psychotherapie-Durchführung (Internet-Psychotherapie), Psychologische Beratung per E-Mail-Austausch – Absenden und Empfangen – immer mit Verschlüsselung.
- 📧 Ein **Virenschutz-Programm** installieren, automatisch Updates lassen und permanent nutzen, auch beim Absenden. (Virenschutz plus Spyware-Schutz plus ggf. Phishing-Schutz)
- 📧 E-Mail-Anhänge nur bei Sicherheit über deren Herkunft öffnen, ggf. sogar vorher beim Absender nachfragen. Die „Autovorschau“ bewirkt bereits „Öffnen“ der E-Mail, ist abschaltbar.

- ☞ Spam-Filter schützen gegen unerwünschte und lästige E-Mails, indirekt auch vor Schadprogramm-E-Mails.
- ☞ Das Sende- und Empfangs-Format „Nur Text“ (ASCII) mit einfacher Schrift und minimaler Formatierung (auch bei empfangenen E-Mails; nicht im HTML-Format) erhöht die Sicherheit allgemein.
- ☞ Das Aufführen der eigenen E-Mail-Adresse in der Form „Eigener.Name(at)providername.de“ (Ersatz des @-Zeichens durch „at“) auf Webseiten und in E-Mail-Texten selbst schützt gegen automatisches Adressen-Auslesen durch unberechtigte Fremde. Nachteil ist lediglich für andere, diese Adresse neu eintippen zu müssen. „@“ ausschließlich im Adressfeld der E-Mail.
- ☞ Aus technischen Gründen werden E-Mails auf ihrem Weg von allen beteiligten Providern gespeichert. Dort können sie eingesehen, geändert und gelöscht werden. Authentizität (Absender-Echtheit) und Integrität (Unverändert) bleiben offen.
- ☞ Mit der **Elektronischen Signatur** können E-Mails authentifiziert werden, was die Sicherheit bezüglich des Absenders herstellt.
- ☞ Betriebsinterne Verbindungsdaten-Speicherung/-Protokollierung wegen Privat-geheimnisschutz und ggf. geregelte private Nutzung klären. (Betriebsvereinbarung; Mitarbeiter-Datenschutz!)

(D) Berufliche Internet-Nutzung

- 🌐 **Sparsame Dateneingabe** grundsätzlich, z. B. bei Bestellungen, Newsletter-Anmeldungen, bei Suchanfragen, Diskussions-Beteiligungen; **automatische Löschung** der aufgesuchten Seiten („History“, „Chronik“, „zuletzt besuchte Seiten“) beim Herunterfahren – durch entsprechende Browser-Einstellungen.
- 🌐 Wegen der **Vorratsdatenspeicherung** (VDS) im Auftrag des Staates beim (immer) privaten Provider sollte man sich bewusst sein, dass spätere Fahndungsanlässe auch Zufallsentdeckungen ermöglichen sowie später ggf. abgeschwächte Fahndungshürden zu „Treffern“ führen.
- 🌐 **Cookies** (unbemerkt übertragene Dateien, die die Reidentifizierung ermöglichen) nur ausnahmsweise und vorübergehend (z. B. „für die aktuelle Sitzung“) zulassen durch die entsprechende Browser-Einstellungen, automatische Formular-Eingabe deaktivieren. (Auch aktivierte Suchmaschinen-Toolbars protokollieren das Surfverhalten.)

- 
Firewall installieren, automatisch updaten lassen und permanent nutzen. Diese schützt auch vor Missbrauch des eigenen PC als aktive Quelle in einem Bot-Netz, von wo aus Daten, Dateien und Schad-Programme unbemerkt versandt werden.
- 
 Vor **Downloads** sich der Zuverlässigkeit der Quelle vergewissern.
- 
WLAN-Technik sollte überhaupt nicht oder nur ausreichend gesichert (z. B. mit WAP2) gegen Zugang über ein fremdes Netz und gegen Fremdnutzung des eigenen Netzes genutzt werden: Zugangs-Passwort vor der ersten Verbindung selbst einrichten und regelmäßig ändern. Router auch ganz abschalten. Auch die Nutzung von **Hot Spots** sollte höchst vorsichtig erfolgen; manuelle Verbindungsherstellung, Provider ggf. bewusst aussuchen, Verbindung möglichst kurzzeitig lassen oder gelegentlich unterbrechen.
- 
 Einige **Suchmaschinen und viele Webseiten-Anbieter speichern** ganz ohne oder mit einem unzutreffenden Hinweis auf diese Tatsache die IP-Adressen (Log Files), die von diesen aufgesuchten Webseiten und Suchbegriffe (Problem sind die beauftragten „Statistikersteller“, ggf. unter „Datenschutz“ nachzulesen). Auch deswegen ist die Nutzung von **Anonymisierungs-Diensten** bei Recherchen abzuwägen.
- 
 Bezahldienste und Internet-Banking setzen **verschlüsselte Übertragung** voraus, zu erkennen an der Web-Adresse mit https:// beginnend.
- 
Sozial-Netzwerke / Web 2.0 nur mit überlegter Dateneingabe nutzen; selbst bei Löschung der eigenen Daten werden ggf. schon Kopien andernorts gespeichert (außerhalb deutschen Datenschutz-Rechts; Online-Archive), die von Suchmaschinen auch später noch gefunden werden.
- 
 Bei eigenen **Websites** und Blogs die Datensparsamkeit und ggf. Copyright beachten, eigene Texte unproblematisch.
- 
 Testangebote zum **Selbstdatenschutz** nutzen – z. B. für Browser beim BSI (<http://www.bsi-fuer-buerger.de/browser/browsercheck.htm>), für E-Mail beim [niedersachsen.de](http://www.niedersachsen.de) und fürs Netzwerk. Oder praktische Einübung via <http://www.irbi.de> der L-M-Universität München mit Microsoft – ebenfalls kostenlos, anonym und psychologisch erarbeitet.

- 🌐 Zur Sicherheitserhöhung können „Aktive Inhalte“ (ActiveX-Steuerelemente) und „Javascript“ deaktiviert werden, letzteres kann allerdings Website-Anzeigen beeinträchtigen.
- 🌐 **Aufmerksamkeit** (Awareness) ist durchgehend zu aufzubringen, auch mit Virenschutz und Firewall – eine individuelle „Argwohn-Einstellung“ ist beizubehalten, auch mit Abschirmungs- und Sicherungs-Aktivitäten durch hauptamtliche „EDV-Leute“ in Einrichtungen. Die Wahrnehmung veränderter, betrügerischer Websites, veränderter Eingabeseiten u. ä. kann ausschließlich persönlich-subjektiv erfolgen. Die technischen Vorkehrungen allein reichen nicht aus.
- 🌐 Die **Anwendungs-Schulung** ist gleichermaßen wie die **Anwendungs-Motivierung** kontinuierlich zu kommunizieren und sicherzustellen, sofern in Einrichtungen mehrere Personen in einem PC-Netz tätig sind. Die selten sichtbaren Folgen unzureichender Sicherung und Sorgfalt erschweren bekanntermaßen das Motivieren für das erforderliche **Sicherheitsbewusstsein** gegen Irrtümer und Nachlässigkeiten, die Compliance für sicheres Alltags- und Gewohnheits-Handeln. Die Grenze zwischen geeigneten Selbsthilfe-Aktivitäten und erforderlichen Hilfeanfragen ist zu vermitteln.
- 🌐 **Betriebsinterne Verbindungsdaten-Speicherung/-Protokollierung** wegen Privatgeheimnisschutz und ggf. geregelte private Nutzung sind zu klären und offen zu legen. (Betriebsvereinbarung; Mitarbeiter-Datenschutz)
- 🌐 Software-Updates, sog. Patches, downloaden für alle wesentlichen Kommunikations-Programme: „Automatisches Updaten“ unter Einstellungen einschalten oder manuell regelmäßig veranlassen. Ggf. auch Upgrades – Verbesserungen eines gesamten Programms – herunterladen.

Zusammengestellt aus verschiedenen Datenschutz-Merkblättern, Berichten und Referaten (Quellenangaben): Unabhängiges Landeszentrum für Datenschutz (ULD; Schleswig-Holstein): u. a. „Aktion Datenschutz ... 2006“; mittelstand-sicher-im-internet.de, 2006; Berufs-/Datenschutz-Regel-sammlungen vom LfD Niedersachsen 2004 (zusammen mit der LPK Niedersachsen); LfD NRW: „Schützen Sie Ihre Daten“ 2006; LfDI NRW 2002: „Orientierungshilfe E-Mail und Internet am Arbeits-platz“; weitere LfD-Drucksachen; Sewecom Mainz: „Sicherheitstips für den PC“ 2006; „12 goldene Regeln der PC-Nutzung“ von Stop1984.com; Bundesamt für Sicherheit in der Informationstechnik (BSI): diverse Drucksachen, „Verantwortlichkeiten ...“ 2007, Kap. „Schützen – aber wie?“ und „Abzocker und Spione“ 2007; Heise-Verlags-Pressemitteilungen kontinuierlich, z. B. heise.de/newsticker und heise Security News; Xamit-Sudie: „Wissen Sie, was Sie tun?“... 2007; Berufsverband der Datenschutz-beauftragten Deutschlands (BvD e. V.): Checkliste 2008; Datenschutz und Datensicherheit 7/2007: Schwerpunkt Security Awareness; weitere Einzel-Informationen siehe tws. die Beiträge im REPORT PSYCHOLOGIE und im BDP-Newsletter seit 2005.

Datei: GrMerkbl-PC+IT-beruf1-Nutzung-Hinweise-Sammlg-09vi2.rtf, DrD 08.04.2010-4