



Verschwiegenheitsverpflichtung und Datenschutzbestimmungen für IT-technische Betreuungsarbeiten durch ComNet

Vereinbarung
zwischen dem / der

- Nachstehend „Auftraggeber“ genannt -

Und der
ComNet Computer im Netzwerk Vertriebs GmbH
Carlo-Schmid-Str. 15
52146 Würselen
Tel.: +49 (0)2405 / 4888 - 0
eMail: info@comnet.de

Amtsgericht Aachen: HRB 4463
Geschäftsführer: Holger Schmitz, Benedikt Kisner
- Nachstehend „Auftragnehmer“ oder „ComNet“ genannt -
„Auftraggeber“ und „Auftragnehmer“ werden auch einzeln bzw. gemeinsam nachstehend „Vertragspartner“ genannt.

Stand 01.01.2020

I. Präambel

1. Datenschutz hat die höchste Stufe in der ComNet Compliance! Alle ComNet-Mitarbeiter werden ständig angehalten, jegliches Tun und Handeln vorher diesem Datenschutz-Kodex zu unterziehen. Diese Verschwiegenheitsverpflichtung gilt nicht nur für personenbezogene Daten, sondern auch für alle Unternehmensdaten des Auftraggebers.
2. ComNet - u.a. spezialisiert auf die IT-Betreuung von Kanzleien - ist bekannt, dass bestimmte Berufsgruppen, speziell die Angehörigen des steuerberatenden, wirtschaftsprüfenden und rechtsberatenden Berufes besondere Verschwiegenheitspflichten im Hinblick auf die bekannt gewordenen Tatsachen ihrer Mandanten unterliegen (u.a. § 203 - StGB, §§ 2 ff der Berufsordnung für Rechtsanwälte – BRAK, §§ 43 ff der Bundesrechtsanwaltsordnung – BRAO, §§ 57 ff und §§ 62 ff des Steuerberatergesetzes – StBerG, §§ 43 ff und §§ 50 ff des Gesetzes über die Berufsordnung der Wirtschaftsprüfer – WPO – SGB I, §§ 35 ff des Sozialgesetzbuches usw.).
3. ComNet erklärt außerdem, dass Bestimmungen zur Wahrung des Datengeheimnisses personenbezogener Daten nach Art. 29 der EU-Datenschutzgrundverordnung (EU-DSGVO), Gesetz zur Anpassung des Datenschutzrechts, sog. Datenschutz-Anpassungs-und-Umsetzungsgesetz - DSAnpUG (oft auch BDSG-Neu genannt), die Datenschutzregeln der §§ 91 ff. des Telekommunikations-gesetz (TKG), weiterhin des Fernmeldegeheimnisses aus § 88 TKG sowie die Geheimhaltungsverpflichtungen wettbewerbsrelevanter Daten, insbesondere gemäß § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG), bekannt sind.
4. Es ist weiterhin bei ComNet und seinen Mitarbeitern bekannt, dass bei Verstößen gegen die Vorschriften zum Datenschutz oder gegen das Fernmeldegeheimnis Sanktionen, insbesondere Geldbußen oder Freiheitsstrafen (Art. 843, 844 EU-DSGVO, § 17 UWG, § 206 StGB) verhängt werden können.
5. ComNet bestätigt hiermit außerdem, dass ComNet und ihren Mitarbeitern der § 202a des Strafgesetzbuches (StGB) „Auspähen von Daten“, § 202b StGB „Abfangen von Daten“, § 206 StGB „Verletzung des Post- oder Fernmeldegeheimnisses“, § 263a StGB „Computerbetrug“, § 303a StGB „Datenveränderung“, § 303b StGB „Computersabotage“ bekannt sind.
6. Begrifflichkeiten dieser Verschwiegenheitsverpflichtung werden im Anhang dieser Vereinbarung erklärt.

II. Verpflichtungen:

1. Zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) werden der Auftraggeber und ComNet alle im Rahmen der Geschäftsbeziehung bekannt gewordenen Betriebs- und Geschäftsgeheimnisse beidseitig vertraulich behandeln. Betriebs- und Geschäftsgeheimnisse sind dabei im Zusammenhang mit der Geschäftsbeziehung stehende Umstände oder Vorgänge, die nur einem begrenzten Kreis bekannt, für Außenstehende aber ggfs. Wissenswert sind, die offensichtlich oder nach dem bekundeten Willen des Betriebs- oder Geschäftsinhabers aber geheim zu halten sind und deren Kenntnis durch Außenstehende dem Geheimnisschutzträger zu einem Nachteil gereichen können (hierzu gehören vor allem technische Lösungen, Geschäftsprozesse, Vertragsinhalte, Kundenbeziehungen oder Informationen über Personal und Mitarbeiter). Diese Pflicht bleibt auch nach Beendigung der Geschäftsbeziehung bestehen, es sei denn, dass ein Dritter diese offen offenbart hat.

2. ComNet erklärt, dass die Bestimmungen zur Wahrung des Datengeheimnisses personenbezogener Daten nach der EU-Datenschutzgrundverordnung (EU-DSGVO) und des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 unter Umsetzung der Richtlinie (EU) 2016/680 (sog. „Datenschutz-Anpassungs-und-Umsetzungsgesetz EU“ – DSAnpUGEU oder oft auch „BDSG-Neu“ genannt) strikt eingehalten werden.

Ergänzend zu dieser Verschwiegenheitsverpflichtung schließen der Auftraggeber und ComNet noch eine separate „Vereinbarung zur Auftragsverarbeitung“ gemäß Art. 28 EU-Datenschutzgrundverordnung (EU-DSGVO) ab.

3. ComNet sichert zu, dass ComNet für die Erbringung von Dienstleistungen nur geschultes Personal einsetzen wird, das mit den Bestimmungen zum Datenschutz, zur Datensicherheit und den berufsspezifischen Verschwiegenheitsverpflichtungen vertraut und geschult ist.

4. ComNet wird in geeigneter Form alle Mitarbeiter, die ComNet im Rahmen der Auftragserfüllung einsetzt, auf das Erfordernis außerordentlicher Vertraulichkeit hinweisen und auf die besonderen Verschwiegenheitspflichten und das Datengeheimnis einmal jährlich verpflichten und schulen.

ComNet hat einen externen Datenschutzbeauftragten bestellt, der auf die Einhaltung des Datenschutzes hinwirkt und prüft.

5. ComNet verpflichtet sich, alle Informationen über Betriebs und Geschäftsgeheimnisse des Auftraggebers streng vertraulich zu behandeln und insbesondere den Schutz der zugänglichen bzw. überlassenen Daten durch entsprechende technische und organisatorische Maßnahmen sicherzustellen.

6. Zusatzverpflichtung für Berufsgeheimnisträger (Steuerberater, Wirtschaftsprüfer, Rechtsanwälte usw.) bzgl. der (neuen) Regelung des § 203 StGB zum Schutz von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen:

a. ComNet wirkt als IT-Dienstleister z.Tl. an der beruflichen Tätigkeit des Auftraggebers mit, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt. ComNet wahrt in Kenntnis der strafrechtlichen Folgen einer Verletzung der Verschwiegenheitspflicht gemäß § 203 StGB (Freiheitsstrafe bis zu einem Jahr oder Geldstrafe) und den sonst anwendbaren rechtlichen Vorschriften fremde Geheimnisse, die ihr von dem Auftraggeber zugänglich gemacht werden.

b. ComNet verpflichtet sich, sich nur insoweit Kenntnis von fremden Geheimnissen im Sinne der vorstehenden Position zu verschaffen, als dies zur Vertragserfüllung unbedingt erforderlich ist.

c. ComNet und den ComNet-Mitarbeitern ist bekannt, dass sich die Verschwiegenheitspflicht nicht nur auf fremde Geheimnisse erstreckt, sondern auf alle Tatsachen, die in Ausübung oder aus Anlass der Tätigkeit für den Auftraggeber, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt, anvertraut oder bekannt werden. Hierzu gehört auch schon die Kenntnis, welche Mandate betreut werden.

d. Bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandat oder einer einzelnen Person dienen, ist der Auftraggeber verpflichtet, die Einwilligung des Mandanten in die Zugänglichmachung von fremden Geheimnissen im Sinne dieser Vereinbarung einzuholen.

e. ComNet ist berechtigt, Dritte zur Vertragserfüllung heranzuziehen (z.B. Softwarehersteller wie Microsoft, DATEV, Addison usw.). Beim Einsatz von Dritten verpflichtet sich ComNet, diese in Textform unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, soweit diese im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten.

Sollte es sich um personenbezogene Daten handeln, hat der Auftraggeber nach der „Vereinbarung zur Auftragsverarbeitung nach EU-DSGVO Art. 28 Abs. 2“ ein Ablehnungsrecht und muss vor Beauftragung befragt werden – sofern es sich nicht um einen Unterauftragnehmer handelt, der im Rahmen der Vereinbarung zur Auftragsverarbeitung genehmigt wurde.

f. Die Pflicht zur Verschwiegenheit gemäß den vorstehenden Sätzen dieser Position besteht nicht, soweit ComNet auf Grund einer behördlichen oder gerichtlichen Entscheidung zur Offenlegung von vertraulichen Informationen des Auftraggebers verpflichtet ist/wurde. Soweit dies im Einzelfall zulässig und möglich ist, wird ComNet den Auftraggeber über die Pflicht zur Offenlegung möglichst vorab in Kenntnis setzen.

g. ComNet ist die Rechtslage zu §§ 53a i.V.m. 53, 97 StPO, §§ 383 f ZPO bekannt (Mitwirkung an der beruflichen Tätigkeit eines Auftraggebers, der einer beruflichen Verschwiegenheitsverpflichtung unterliegt). Der o.a. Kreis von Beteiligten wird bei Gerichten und Behörden über Tatsachen, die mit der Tätigkeit bekannt werden, ohne vorherige Genehmigung des Auftraggebers nicht aussagen oder sonst Auskunft erteilen.

7. Bei ComNet besteht die strikte Anweisung, dass für jede Dienstleistungsbeauftragung anschließend ein Serviceschein zur Dokumentation der durchgeführten Arbeiten erstellt wird und dieser dem Auftraggeber unverzüglich zugeleitet werden muss. Der Auftraggeber ist gehalten, die Protokolle (d.h. diese Servicescheine) im Rahmen seiner Geschäftstätigkeit unverzüglich zu überprüfen und zu archivieren. Beanstandungen sind innerhalb von drei (3) Werktagen zu melden.

8. Nach Beendigung der ComNet-Dienstleistungen sind alle Daten entweder unverzüglich physikalisch zu löschen und alle in diesem Zusammenhang entstandenen Kopien, Ausdrucke, Listen, Datenträger und Ähnliches zu vernichten oder auf ausdrücklichen Wunsch des Auftraggebers an diesen zurückzugeben.

Hinweis: Bei Beendigung eines Server-Housing-, IaaS-, ASP-, Cloud- oder sonstigen Rechenzentrums- Vertrages ist ComNet nicht berechtigt, die Daten des Auftraggebers weiter zu verarbeiten. ComNet wird die Löschung innerhalb von neunzig (90) Tagen vornehmen, soweit nichts anderes vereinbart ist. Sofern Leistung gemäß dem Hauptvertrag eine Datenaufbewahrung ist, z.B. eine Archivierung, insbesondere über die Laufzeit einer Verarbeitungstätigkeit hinaus, werden diese Auftraggeber- Daten erst nach Ablauf der vereinbarten Archivierungszeit gelöscht. Wünscht der Auftraggeber eine relativ dazu vorzeitige Löschung, unterbreitet ihm der Auftragnehmer ein Angebot für die Vornahme der Löschungsstätigkeit.

9. Werden Computer, Drucker, Kopierer, Scanner, Monitore, USV, sonst. IT-Geräte, Datenträger, Festplatten, Magnetbänder, sonst. Speichersysteme usw. an ComNet zur Entsorgung gegeben, so sorgt ComNet beim entsprechenden Kauf von Neugeräten für eine Verschrottung gemäß der aktuellen gesetzlichen Elektroschrott-Verordnung (ComNet weist hier darauf hin, dass man keine Verkaufsfläche von mindestens 400 m² hat und somit nicht unter die Verpflichtung nach ElektroG zur kostenlosen Rücknahme fällt).

Die Anlieferung zu ComNet am Standort Würselen hat der Auftraggeber durchzuführen oder ComNet berechnet die Personalaufwendungen und Transportkosten. Wünscht der Auftraggeber den Ausbau von Speichersystemen und eine ordnungsgemäße „datenschutzkonforme“ Entsorgung, Vernichtung und/oder Datenlöschung, so führt ComNet diese Leistungen kostenpflichtig durch und stellt diese Aufwendungen dem Auftraggeber separat in Rechnung.

10. ComNet überprüft vorsorglich die ComNet-eigenen DV-Anlagen und Datenträger ständig auf Virenbefall. Sofern das "Einführen" von ComNet-Datenträgern (z.B. Service-DVDs, USBSticks, Update-CDs/DVDs usw.) in die DV-Anlage des Auftraggebers notwendig werden sollte, sind die ComNet-Mitarbeiter angehalten, vor und nach jeder DV-technischen Betreuungsmaßnahme die DV-Anlage auf Virenbefall zu überprüfen (dies gilt nicht für Original-Programm-/Datenträger von Hard- oder Software-Herstellern). Gleiches gilt für Datenfernübertragungs-Kopplungs-Maßnahmen. Dieser Viren-Check wird im ComNet-Serviceschein protokolliert. Die Arbeitsaufwendungen für den Viren-Check werden dem Auftraggeber nach tatsächlichem Zeitaufwand in Rechnung gestellt, sie sind nicht Bestandteil möglicher ComNet-"Full-Service"-Dienstleistungs-, Gewährleistungs- bzw. Wartungsverpflichtungen. ComNet empfiehlt jedem Auftraggeber auf seinen DV-Anlagen selbst ein leistungsfähiges, kontinuierlich aktualisiertes Viren-Check-Programm einzusetzen und dieses ständig zu aktualisieren.

11. Müssen Geräte, Teile oder komplette DV-Anlagen des Auftraggebers in den Werkstattbereich von ComNet verbracht werden, auf denen sich personenbezogene Daten befinden, ist ComNet verpflichtet diese Bereiche mit einer VdS-anerkannten Alarmanlage auch außerhalb des Geschäftsbetriebes zu überwachen, deren Alarmmeldungen direkt auf einen anerkannten VdS-anerkannten Wach- und Sicherheitsdienst zur 24/7 Überwachung aufgeschaltet ist.

Ergänzend (vorrangig) gelten die "Allgemeinen Geschäftsbedingungen von ComNet", die jederzeit im Internet unter www.ComNet.de/Kundenbereich eingesehen werden können – auf Wunsch schickt ComNet diese gerne auf Anforderung auch zu.

.....
(Ort, Datum)

.....
(Ort, Datum)

.....
(rechtsverbindliche Unterschrift und Stempel des **AUFTRAGGEBERS**)

.....
(rechtsverbindliche Unterschrift und Stempel des **AUFTRAGNEHMERS**)

Anlage A

Begrifflichkeiten

Administration

Der „**Administrator**“ betreut Computersysteme und -netzwerke. Er ist daher Inhaber umfassender Nutzungsrechte („**Admin-Rechte**“). Er plant, installiert, konfiguriert und pflegt die IT-Infrastruktur einer Kanzlei bzw. eines Unternehmens. Hierzu gehören neben Serverfarmen, Workstations, Storage auch Datensicherungen, Router, Netzwerkkomponente, Internet- und Telekommunikations-Anschlüsse.

ASP

„**Application Service Providing**“ (**ASP**) ist eine Dienstleistung, der eine zum Informationsaustausch über ein öffentliches Netz oder über ein privates Datennetz anbietet. Der ASP-Dienstleister (**ASP-Provider**) kümmert sich um die gesamte Administration, wie Datensicherung, das Einspielen von Patches, Updates, Upgrades, die Installation, den Betrieb, die Instandhaltung und Instandsetzung der Server-Farmen, der Storages, der Einwahltechnik usw. Teil der ASP-Dienstleistung ist regelmäßig auch ein Service (z.B. Benutzerbetreuung) rund um die Anwendung. Bei einem ASP-Vertrag wird die benötigte Software nicht gekauft, sondern für die Nutzung werden z.B. bei Microsoft-Programmen **SPLA-Lizenzen (Service-Provider-License-Agreement)** angemietet oder wie im Fall von DATEV-Software vom Anwender beigestellt.

Backup

Unter „**Backup**“ oder „**Datensicherung**“ versteht man das teilweise oder gesamte Kopieren der in einem Computersystem vorhandenen Daten auf ein anderes Speichermedium, um einen Datenverlust bei Systemausfällen zu begrenzen. Die auf dem Speichermedium gesicherten Daten werden als Sicherungskopie oder als Backup bezeichnet. Eine Datensicherung sollte heute mindestens 1 x täglich erfolgen. Es empfiehlt sich sogar, täglich zwei (2) Datensicherungen auf unterschiedliche Speichermedien und mit unterschiedlichen Verfahren durchzuführen. Zudem sollten Datensicherungen in Zeitabständen an einem anderen sicheren Ort außerhalb des Gebäudes, wo sich die Server befinden, aufbewahrt werden.

BDSG-NEU

Das „**Bundesdatenschutzgesetz-NEU**“ (**BDSG-NEU**) wurde als Teil des „**Datenschutz-Anpassungs- und -Umsetzungsgesetz EU**“ (**DSAnpUG-EU**) beschlossen. Diese neueste Fassung des BDSG tritt am 25. Mai 2018 mit der „**EU-Datenschutzgrundverordnung**“ (**EU-DSGVO**) in Kraft und ersetzt das alte BDSG komplett.

BGB

Das „**Bürgerliche Gesetzbuch**“ (**BGB**) ist Teil des Privatrechts, das die Beziehungen zwischen rechtlich gleichgestellten Rechtsteilnehmern (Bürgern, Unternehmen) regelt. Der I. Teil des BGB „**Allgemeiner Teil**“ (**§§ 1-240 BGB**) enthält die wesentlichen Grundregeln, die für das gesamte bürgerliche Recht gelten. Der II. Teil „**Schuldrecht**“ (**§§ 241-853 BGB**) beinhaltet u.a. das Kaufvertragsrecht, das Werksvertragsrecht, das Leihvertragsrecht, das Mietvertragsrecht und das Darlehensvertragsrecht. Bei dem III. Teil „**Sachenrecht**“ (**§§ 854-1296 BGB**) geht es in erster Linie um das Verhältnis von Personen zu Gegenständen ihres Privatvermögens, um Eigentums- und Besitzverhältnisse. Der IV. Teil „**Familienrecht**“ (**§§ 1297-1921 BGB**) regelt die rechtlichen Verhältnisse, die Personen aufgrund von familiären Beziehungen und Ehebindungen zueinander haben. In dem 5. Teil „**Erbrecht**“ (**§§ 1922-2385 BGB**) geht es um die Vermögensverhältnisse nach dem Tod einer Person, Regelungen für Erben, Testament usw. Bei bürgerlich-rechtlichen Gerichtsverfahren werden die Streitigkeiten nach der „**Zivilprozessordnung**“ (**ZPO**) geregelt.

BRAO

Die „**Bundesrechtsanwaltsordnung**“ (**BRAO**) regelt das Berufsrecht der Rechtsanwälte in Deutschland, das heißt die Rechte und Pflichten, die der

BORA	Rechtsanwalt gegenüber Mandanten und Dritten zu beachten hat, sowie diverse weitere berufsrechtliche Fragen. Rechtsanwälte unterliegen der Berufsaufsicht ihrer Rechtsanwaltskammer (Körperschaften öffentl. Rechts). Ergänzend gibt es die „ Berufsordnung für Rechtsanwälte “ (BORA) eine von den gewählten Vertretern der Rechtsanwälte in Deutschland selbst gegebene Berufsordnung, die nähere Einzelheiten zu den beruflichen Pflichten regelt und zum Berufsrecht gehört.
BOSTb	Für den Berufsstand der Steuerberater ist eine selbstaufgelegte „ Berufsordnung für Steuerberater und Steuerbevollmächtigte “ (BOSTb) maßgeblich, die Zweifels- und Auslegungsfragen regelt und darüber hinaus die Grundsätze der Berufsethik festlegt.
Cloud-Computing	„ Cloud-Computing “ beschreibt die Bereitstellung einer IT-Infrastruktur u.a, wie Server, Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet.
DATEV	Die „ DATEV e.G. “ ist eine berufsständische Genossenschaft, bei der nur Steuerberater, Wirtschaftsprüfer und Rechtsanwälte Mitglieder werden können. Nur diese Berufsträger können bisher auch die Produkte der DATEV beziehen. Nur mit Erlaubnis eines Berufsträger-Genossen (wie Steuerberater) können bisher auch Mandanten, wie mittelständische Unternehmen, Kommunen und Institutionen im sogenannten „mitgliedsgebundenen Mandantengeschäft“ die DATEV -Leistungen erhalten und nutzen. Das DATEV -Produktangebot umfasst Software für Finanzbuchführung, Jahresabschluss, Steuerdeklaration, Lohn- und Gehaltsabrechnung, Lösungen für Wirtschaftsprüfer, Rechtsanwälte, Kommunen und kommunale Betriebe, Leistungen für die Datendistribution und Informationsbereitstellung, Sicherheitsdienstleistungen und Consulting.
EU-DSGVO	Die „ Datenschutz-Grundverordnung “ (EU-DSGVO) harmonisiert in der Europäischen Union die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der EU sichergestellt und andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.
IaaS	Unter „ Infrastructure as a Service “ (IaaS) versteht man ein Geschäftsmodell, bei dem ein RZ-Dienstleister IT-Infrastruktur (Server, Speicher usw.) über ein öffentliches Netz oder über ein privates Datennetz anbietet, so dass der Anwender diese Infrastruktur nicht kaufen muss, sondern bei Bedarf (on demand) anmietet.
Login	Die „ Benutzerkennung “ oder das „ Login “ dient der Identifikation eines Anwenders und besteht in der Regel aus Buchstaben, Zahlen und Sonderzeichen.
Passwort	Das „ Passwort “ oder auch „ Kennwort “ genannt, ist eine beliebige, vorgegebene oder vom Nutzer selbst gewählte alphanumerische Zeichenfolge, das der Authentifizierung eines Benutzers dient. Passwörter kommen in Verbindung mit einer Benutzerkennung oder Login zum Einsatz. Passwörter sollten heutzutage aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen und 8 Zeichen lang sein. Passwörter müssen geheim gehalten werden und dürfen nicht an Bildschirmen oder auf/unter Tastaturen usw. angebracht sein.
Private Cloud	Eine „ Private Cloud “ ist eine Rechenzentrumsleistung bzw. RZ-Umgebung die zwar über ein öffentliches Netz oder über ein privates Datennetz erreichbar ist, auf die aber ausschließlich ein Unternehmen, eine Kanzlei, eine Organisation Zugriff hat (Beispiel: Kanzlei- oder Unternehmens-ASP-System).

Public Cloud	Im Gegensatz zur „Private Cloud“ bietet die „ Public Cloud “ den Zugang zu öffentlichen, für Jedermann zugänglichen IT-Infrastrukturen über das Internet (Beispiel: Amazon-Bestellshop, Bahn-, Flug-, Reise- Portale, Facebook, Xing usw.). Die „ Hybride Cloud “ kombiniert die beiden Cloud-Möglichkeiten Public- und Private-Cloud.
Server-Housing	„ Server-Housing “ bedeutet die Unterbringung und Netzanbindung von gekauften oder gemieteten Server-Farmen und Storages in einem Rechenzentrum eines „ Internet Service Providers “ (ISP).
StBerG	Das „ Steuerberatungsgesetz “ (StBerG) ist das Gesetz, das die Steuerberatung in Deutschland regelt. Steuerberater unterliegen der Berufsaufsicht ihrer jeweiligen Steuerberaterkammer (Körperschaften öffentl. Rechts).
SGB I	Das „ Sozialgesetzbuch Erstes Buch “ (SGB I) oder das Erstes Buch Sozialgesetzbuch stellt grundsätzliche Regelungen zur sozialen Sicherheit in Deutschland auf. Die sozialen Rechte, die einzelnen Sozialleistungen und die zuständigen Sozialleistungsträger werden benannt.
StGB	Das „ Strafgesetzbuch “ (StGB) regelt in Deutschland die Kernmaterie des materiellen Strafrechts. Während es dazu die Voraussetzungen und Rechtsfolgen strafbaren Handelns bestimmt, ist das Verfahren zur Durchsetzung seiner Normen, d.h. das Strafverfahren, in der „ Strafprozessordnung “ (StPO) geregelt.
TKG	Das „ Telekommunikationsgesetz “ (TKG) regelt bzw. reguliert in Deutschland den Wettbewerb im Bereich der Telekommunikation.
UWG	Das „ Gesetz gegen den unlauteren Wettbewerb “ (UWG) schützt Mitbewerber, Verbraucher und die Allgemeinheit vor einer unfairen Wettbewerbsverzerrung. Das UWG gewährt u.a. Unterlassungs-, Schadensersatz-, Beseitigungs-, Gewinnabschöpfungs- und Auskunftsansprüche.
WdS	VdS war ursprünglich die Abkürzung für „ Verband der Schadenversicherer “. Heute ist die „VdS Schadenverhütung GmbH“ ein Unternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. und in die Bereiche Brandschutz, Security (Einbruchschutz), Cyber-Security (Informationssicherheit), Naturgefahren und Managementsysteme unterteilt. Das VdS Zertifikat ist das Gütesiegel ein Qualitätshinweis beim Betrieb von Sicherheitstechnik und Sicherheitsdienstleistungen.
VoIP	Als „ Voice over Internet Protocol “ bezeichnet man die Telefonie über Computernetzwerke, die nach dem Internet-Standard aufgebaut sind. Es können sowohl über Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung ins Netz herstellen. Wichtig: Daten sind leichter abhörbar, als über eine klassische ISDN-Leitung und die Qualität ist auch im Allgemeinen schlechter. Damit die Sprache nicht „zerhackt“ ankommt, muss das Netzwerk (Switches, Router usw.) mit „Quality-of-Service“ ausgestattet sein, um die VoIP-Telefongesprächen priorisiert zu übertragen.
VPN	Ein „ Virtuelles privates Netzwerk “ (VPN) ist ein logisches Netzwerk, bei dem zwei IT-Systeme räumlich voneinander getrennt über einen verschlüsselten IP-Tunnel miteinander verbunden sind.
WPO	Die „ Wirtschaftsprüferordnung “ (WPO) regelt das Berufsrecht der Wirtschaftsprüfer und der vereidigten Buchprüfer. Wirtschaftsprüfer und vereidigte Buchprüfer unterliegen der Berufsaufsicht der Wirtschaftsprüferkammer (Körperschaft öffentl. Rechts).