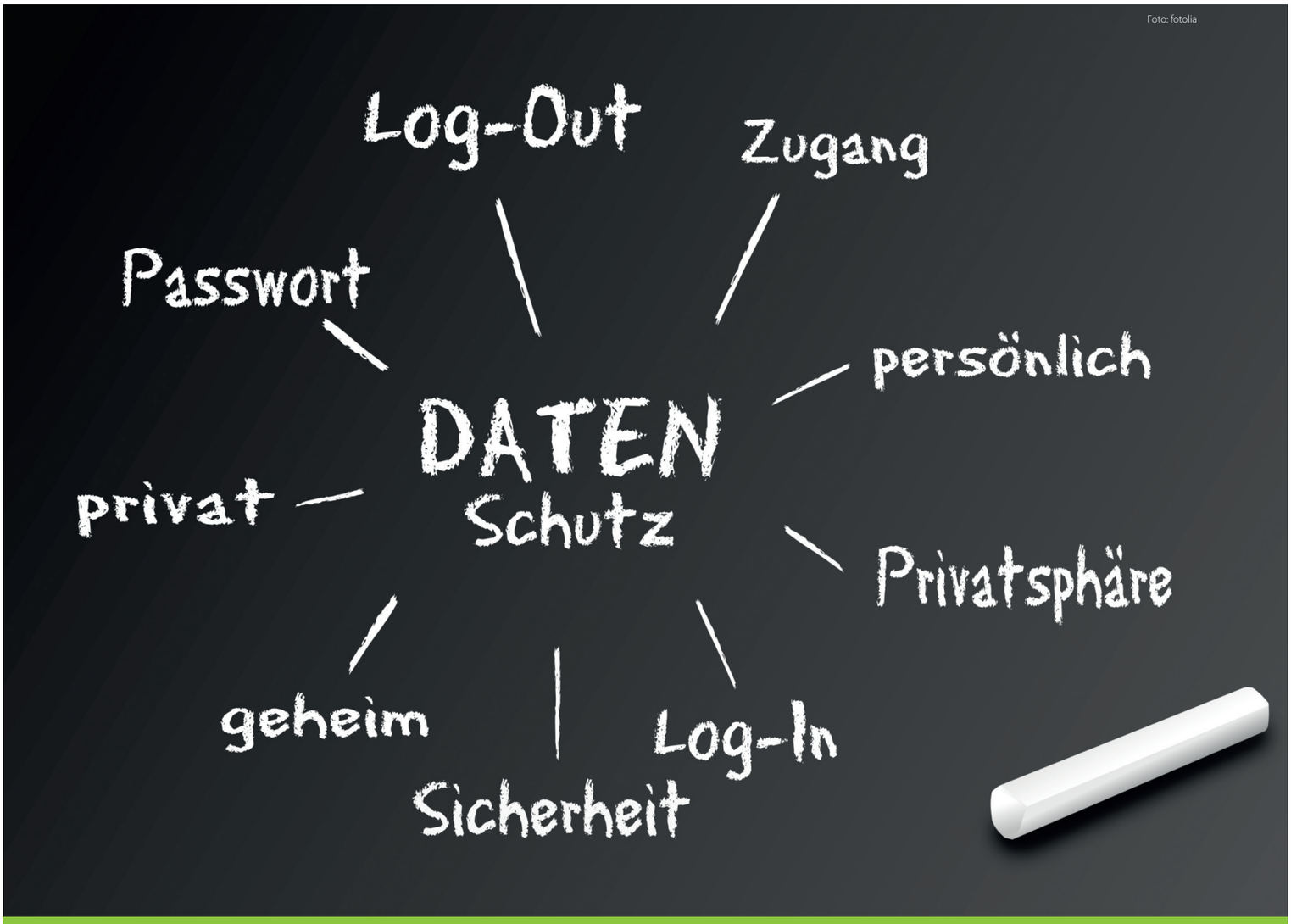

Foto: fotolia

Daten- und Geheimnisschutz

Doppeltes Muss für Übersetzer und Dolmetscher

Sprachmittler haben bei ihrer Arbeit mit vielfältigen schützenswerten Daten und Informationen zu tun. Für Einzelübersetzer und -dolmetscher, denen kein geschulter Datenschutzbeauftragter zur Seite steht, ist es nicht immer einfach, innerhalb des Regelungsdickichts den Überblick zu behalten und die richtigen Maßnahmen zu ergreifen. Zumal nicht nur die Technik Risiken birgt.

0404_Datenschutz_Uebersetzer.indd 10 31.08.2011 10:16:18 Uhr

Auf den ersten Blick scheint es ganz klar: Der Datenschutz ist gesetzlich geregelt, und für Betriebs- und Geschäftsgeheimnisse gilt die Verschwiegenheitspflicht, wie sie in § 5 der Berufs- und Ehrenordnung des BDÜ festgeschrieben ist. Auf beides gewissenhaft zu achten, ist für Sprachmittler nicht zuletzt auch eine Frage der Existenz. Denn: Die Verletzung von Gesetzen, die dem Schutz von Geheimnissen oder personenbezogenen Daten dienen, kann erhebliche Sanktionen nach sich ziehen. So sieht das Bundesdatenschutzgesetz bei Zuwiderhandlung gegen die datenschutzrechtlichen Bestimmungen Bußgelder bis zu 300.000 Euro oder Haftstrafen bis zu zwei Jahren oder Geldstrafen vor. Verstöße gegen Geheimhaltungspflichten können noch schärfere Sanktionen nach sich ziehen.[1] Im schlimmsten Fall droht bei Landesverrat in einem besonders schweren Fall lebenslange Freiheitsstrafe. Vertragsstrafen oder zivilrechtliche Schadensersatzansprüche können erhebliche bis gar existenzgefährdende Ausmaße annehmen – ganz zu schweigen vom Imageschaden, der mit dem Bekanntwerden eines Datenschutzvergehens verbunden ist.

Unsicherheit, Unkenntnis und Unbedachtsamkeit

Das Problem: Für den Daten- und Geheimnisschutz bzw. zu den zivil- und strafrechtlichen Haftungstatbeständen gelten eine Vielzahl von Bundes- und Landesgesetzen oder Rechtsverordnungen, die zudem durch viele unbestimmte Rechtsbegriffe und unübersichtliche Ausnahmen und Rückausnahmen für Laien kaum noch verständlich sind. Also schauen wir einmal genauer hin: Was fällt denn nun unter den gesetzlich geregelten Datenschutz, und wo lauern die (nicht selten unterschätzten) Gefahren des ungewollten Verrats von Betriebs- und Geschäftsgeheimnissen?

Datenschutz

Sinn und Ziel des Datenschutzes ist es, den Einzelnen in seinem Persönlichkeitsrecht zu schützen, wenn andere – in welcher Art auch immer – mit seinen Daten umgehen. Daher hat jeder grundsätzlich das Recht, darüber zu entscheiden, wem er seine Daten zu welchem Zweck offenbart. Ohne die Einwilligung des Betroffenen oder eine gesetzliche Berechtigung oder Verpflichtung darf keine Stelle die Daten erheben, verarbeiten (darunter zählt im Datenschutzrecht vor allem: speichern, verändern, löschen, übermitteln) oder in sonstiger Weise nutzen. Es gibt – wie so häufig im Recht – Ausnahmen von diesem „Verbot mit Erlaubnisvorbehalt“: So darf man natürlich das private Adressbuch auch ohne Einwilligung der Freunde und Bekannten pflegen.

Sprachmittler haben mit vielfältigen Arten dieser Daten zu tun. Zum einen sind dies die Daten ihrer Kunden (insbesondere Vertrags-, Abrechnungs-, Kontaktdaten) und Kooperationspartner (Berufskollegen, Lektoren etc.). Dann finden sich – je nach Ausrichtung der sprachmittlerischen Tätigkeit – personenbezogene Daten in den zu übersetzenden oder zu dolmetschenden Texten. Der Umgang der Sprachmittler mit solchen Daten, also auch das Übertragen in eine andere Sprache, fällt grundsätzlich unter das Datenschutzrecht. Jedes Unternehmen, also auch ein freiberuflich tätiger Sprachmittler, unterliegt als sogenannte verantwortliche Stelle den Vorschriften der Datenschutzgesetze.

Personenbezogene Daten

Personenbezogene Daten im Sinne des Datenschutzrechts sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Darunter fallen Angaben wie z. B. Name, Alter, Anschrift, Staatsangehörigkeit, Beruf, Einkommen sowie die – datenschutzrechtlich als besonders sensibel eingestuften und daher besonders zu schützenden – Daten über die rassische und ethnische Herkunft, über politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Personenbezogen sind die Daten auch dann noch, wenn – eventuell unter Zuhilfenahme anderer Informationen – auf eine bestimmte Person geschlossen werden kann, auch wenn ihr Name nicht genannt ist.

Es gibt keine unwichtigen Daten

Gerade mit den heutigen Möglichkeiten, Daten massen- und dauerhaft elektronisch zu speichern, blitzschnell zu übermitteln, zusammenzuführen, fast beliebig miteinander zu kombinieren und auszuwerten, kann jedes Datum eine für den Betroffenen erhebliche negative Relevanz haben bzw. bekommen. Beispiel: Die Angabe in einer Geburtsurkunde, wo jemand geboren ist, hat für sich genommen vielleicht keine besondere Bedeutung. Diese kann sie jedoch erhalten, wenn es in einer Straftaten-Statistik heißt, dass ein Delikt vornehmlich von Personen aus einer bestimmten Gegend verübt wird.

Für den Betroffenen genauso fatal ist, dass eventuell auch falsche oder veraltete Daten einfließen und so womöglich ein verzerrtes Bild von der Persönlichkeit erstellt

1 Vgl. hierzu: Cebulla, Manuel: Sprachmittlerstrafrecht. Die strafrechtliche Verantwortlichkeit der Dolmetscher und Übersetzer. Berlin 2007, S. 72–108 (erhältlich bei der BDÜ Weiterbildungs- und Fachverlagsgesellschaft mbH).

0404_Datenschutz_Uebersetzer.indd 11 31.08.2011 10:16:18 Uhr

wird, auf dessen Grundlage dann weitreichende Entscheidungen getroffen werden, z. B. über die Bonität einer Person oder das mit ihr verbundene Versicherungsrisiko – mit der Folge, dass ein Versicherungsantrag eventuell zurückgewiesen wird oder es einen Kredit nur zu einem erhöhten Zinssatz gibt.

Betriebs-, Geschäfts- und Staatsgeheimnisse

Neben Daten, die unter das Datenschutzrecht fallen oder als Privatgeheimnisse auch vom Strafgesetzbuch geschützt werden, kommen Sprachmittler mit den unterschiedlichsten Informationen ihrer Kunden oder Dritter in Berührung, die als Betriebs-, Geschäfts- oder Staatsgeheimnisse ebenfalls geschützt werden müssen und die ebenso vielfältigen Gefahren ausgesetzt sind. Neben den üblichen kriminellen Angriffen mit Schadprogrammen, die zur Zerstörung von Daten führen und gegen die sich jeder Computernutzer schützen muss, können Sprachmittler ein interessantes Ziel für Wirtschaftsspionage und Konkurrenzausspähung darstellen.

Spionage: die reale Gefahr

Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von ausländischen Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen. Der Verfassungsschutz nennt in seinen Publikationen beispielhaft russische und chinesische Geheimdienste.[2] Mit den ausspionierten Informationen werden Unternehmen mit Know-how oder auch mit Informationen zu aktuellen Teilnahmen an Ausschreibungen versorgt. Konkurrenzausspähung hingegen ist die Ausforschung eines Unternehmens durch einen Wettbewerber.

Seit Anfang April 2011 arbeitet das Cyber-Abwehrzentrum des Bundesamtes für Sicherheit in der Informationstechnik zum Schutze der staatlichen Infrastruktur. In einer Meldung von Heise-Online vom 18. 5. 11 hieß es, dass die Bundesregierung täglich rund fünf Cyberangriffe aus dem Ausland auf die staatliche Infrastruktur stoppe. Dass ausländische Geheimdienste dahinterstecken, sei in vielen Fällen wahrscheinlich.

Schadsoftware aus dem Internet sehen nach einer jüngst durchgeführten Studie 97 % der betrieblichen Sicherheitsmanager als ernst zu nehmendes Risiko.[3] 96 % fürchten, dass Angreifer die betriebliche IT gezielt schädigen wollen. 53 % der Befragten schätzen solche Angriffe als hohes Risiko ein, gefolgt von Datendiebstahl (44 %) und Konkurrenzausspähung bzw. Wirtschaftsspionage (43 %). Dabei handelt es sich um reelle Sorgen. Das zeigt die Tatsache, dass 69 % der befragten betrieblichen Sicherheitsmanager in den beiden vorausgegangenen Jahren mit mindestens einem Fall von Cybercrime konfrontiert waren.

Wie Sprachmittler Ziel von Spionage werden können

Sprachmittler können zum einen Ziel von direkten Spionageversuchen werden, also von direktem Ausspähen von Ausgangstexten, Übersetzungen und Referenzmaterialien des Kunden auf dem Rechner, im E-Mail-Postfach oder im Büro des Sprachmittlers.

Daneben „eignen" sich Sprachmittler auch für Social Engineering – nicht zuletzt, weil sie durch ihre Arbeit und ggf. auch private Aktivitäten auf elektronischen Plattformen eine Reihe von verräterischen Spuren hinterlassen, die Ausgangspunkt für Spionage- oder Social-Engineering-Aktivitäten werden können.

Social Engineering und Identitätsdiebstahl

Social Engineering wird zunehmend genutzt, um Zugang zu sensiblen Informationen oder Bereichen eines Unternehmens oder einer Behörde zu erlangen: Unter Ausnutzung menschlich-sozialer Verhaltensweisen wie Hilfsbereitschaft, psychologischer Tricks und geschickter Fragen entlocken Angreifer dem Sprachmittler die für sie relevan-

So schützen Sie sich vor Social Engineering und Identitätsdiebstahl

- Treffen Sie klare Regelungen, um einen unbeabsichtigten Informationsfluss zu verhindern, nicht nur mit (Ehe-)Partner und Kindern, sondern auch mit Kollegen im Projekt.
- Hegen Sie ein gesundes Misstrauen.
- Fragen Sie Anrufer nach Namen und Rückrufnummer und prüfen Sie die Angelegenheit, bevor Sie zurückrufen und Informationen erteilen.
- Lernen Sie die Stimmen der befugten Kommunikationspartner in einem Telefonat kennen, um vorgetäuschte Anrufe besser erkennen zu können.
- Sprechen Sie mit Ihren Kunden zu Beginn des Projekts oder der Zusammenarbeit die Kanäle und das Verfahren ab, über die bzw. wie kommuniziert wird.
- Seien Sie mit Informationen über Ihre konkrete Arbeit – auch gegenüber Freunden und Verwandten – sehr sparsam. Auch Freunde, Partner oder Kinder können Einfallstore für Spionageaktivitäten sein.

2 Vgl. beispielsweise Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern (Hg.): Wirtschaftsspionage. Risiko für Ihr Unternehmen. Köln, 2008, S. 10.

3 Vgl. Sicherheits-Enquête 2010/11 der WIK – Zeitschrift für die Sicherheit der Wirtschaft, Ausgabe April 2011.

0404_Datenschutz_Uebersetzer.indd 12 31.08.2011 10:16:19 Uhr

ten Informationen oder Angaben, mit denen sie dann an anderer Stelle im Zielunternehmen an weitere Informationen gelangen. So könnten Sprachmittler – ohne es zu bemerken – über Angelegenheiten ihrer Auftraggeber ausgehorcht werden, die eigentlich vertraulich sind.

Zu den gängigen Methoden zählt es beispielsweise, die Betroffenen unter Stress zu setzen. Folgendes könnte sich ereignen: Bei Tochter oder Sohn einer Übersetzerin meldet sich ein Anrufer und gibt sich als Mitarbeiter des Unternehmens aus, für das sie gerade eine technische Spezifikation übersetzt, und sagt: „Ich kann Ihre Mutter gerade nicht erreichen und brauche unbedingt die Rohfassung ihrer Übersetzung, an der sie gerade für uns arbeitet. Sie kommen doch an ihren Rechner. Bitte schauen Sie nach dem Dokument und schicken es uns. Es ist sehr dringend."

In Frage kommt auch Identitätsdiebstahl. Erfährt ein Angreifer zu vieles über Ihre Person und Ihre Arbeit, kann er sich gegenüber dem Unternehmen, für das Sie dolmetschen oder übersetzen, als Sie ausgeben und um „erneute" Übersendung von Unterlagen an eine andere E-Mail-Adresse oder um zusätzliche Informationen bitten.

Sprachmittler als unfreiwillige Informanten

Auf verschiedene Art und Weise kann aus den Aktivitäten von Sprachmittlern auf deren Kunden oder Übersetzungsprojekte geschlossen werden, was sie zum lohnenden Objekt für Ausspähung oder Social Engineering macht. Bei vielen Tätigkeiten hinterlassen Sprachmittler wertvolle Spuren, so z. B. bei der Nutzung des Internets. Jede Suche nach einer Information – sei es auf einer Website, über eine Suchmaschine oder in einem Online-Wörterbuch – hinterlässt eine Spur im Netz. Durch Zusammenführen solcher Informationen lässt sich ermitteln, in welchem Bereich oder gar für welchen Kunden ein Übersetzer gerade übersetzt oder auf welchen Einsatz sich ein Dolmetscher vorbereitet.

Übersetzt man vornehmlich Zeugnisse oder Personenstandsurkunden, Werbebroschüren oder Internetseiten etc., wird die Gefahr eines gezielten Ausspionierens eher gering sein. Handelt es sich indes um Ausschreibungsunterlagen für große Industrieprojekte, Handbücher von noch nicht auf dem Markt erschienenen High-Tech-Produkten, Dokumente für eine Patentanmeldung, Spezifikationen von Waffensystemen oder Ähnliches, ist die Gefährdung deutlich größer. Aber auch an innovativen Projekten von mittelständischen Unternehmen besteht großes Interesse, was die in den letzten Jahren zunehmenden ausländischen Spionageangriffe auch auf kleine und mittlere Unternehmen verdeutlichen.

So erschweren Sie, dass über Sie und Ihre Arbeit ein differenziertes Persönlichkeitsprofil erstellt und Informationen ausgewertet werden können

- Nutzen Sie nicht nur eine einzige Suchmaschine.
- Verwenden Sie Suchmaschinen, die sicherer sind als Google oder Bing, z. B. www.ixquick.de, www.startpage.com, www.copernic.com.
- Vermeiden Sie lang andauernde Suchen nach vielen Begriffen hintereinander und melden Sie sich zwischendurch aus dem Internet ab und wieder an.
- Löschen Sie die Suchhistorie.
- Wenn Sie im Internet surfen oder Suchmaschinen nutzen, sollten Sie nicht gleichzeitig bei Google-Mail, Facebook oder bei anderen Diensten persönlich angemeldet sein. Dadurch erschweren Sie es anderen, den Bezug zu Ihrer Person herzustellen.
- Sind Sie in besonders sensiblen Bereichen tätig, sollten Sie zudem während Ihrer Recherchen im Internet Anonymisierungsdienste in Anspruch nehmen, um es noch schwerer zu machen, dass auf Ihre Person geschlossen werden kann.

Aufschlussreiche Spuren

Vielfältige Hinweise über die konkrete Arbeit eines Sprachmittlers ergeben sich auch aus den Angaben, die Sprachmittler in sozialen Netzwerken, Übersetzerforen etc. machen. Auch sollte bei Übersetzerstammtischen nicht zu sehr aus dem Nähkästchen geplaudert werden. Gleiches gilt für die Teilnahme an Konferenzen und den Besuch von Fachmessen, wo man es zudem noch mit gänzlich Unbekannten zu tun hat.

Auch die Website des Sprachmittlers verrät interessante Details, z. B. die Nennung von Fachgebieten und Referenzkunden. Auch hier kann weniger mehr sein.

Die von den Kunden erhaltenen oder vom Sprachmittler selbst angefertigten Terminologielisten und ebenso die ins Rechtschreibprüfungsprogramm aufgenommenen Sonderbegriffe können für Ausspähaktivitäten ebenfalls interessant sein. Daher sollten auch diese entsprechend geschützt werden. Zu beachten ist, dass Terminologien und Glossare Betriebsgeheimnisse darstellen können.

Doch nicht nur das Internet ist eine Schwachstelle, über die Fremde an Informationen kommen können. So senden beispielsweise bestimmte Multifunktionsgeräte – also Geräte mit Drucker, Fax, Scanner in einem – unbemerkt Daten an fremde Server. Und: Bei Standardsoftware oder spezieller Übersetzungssoftware weiß man nicht, was diese Programme neben den gewünschten Funktionalitäten auf den Rechnern tun – und an wen sie welche Daten weitergeben.

0404_Datenschutz_Uebersetzer.indd 13 31.08.2011 10:16:19 Uhr

Verschwiegenheit – und umfassender technischer Schutz

Viele und sehr komplexe Vorschriften und die allgemeine vertragsrechtliche Pflicht zur Rücksichtnahme auf die Interessen und Rechte des Vertragspartners zwingen den Sprachmittler dazu, mit den Daten und Informationen seiner Kunden äußerst sorgsam umzugehen. Das zivil- und auch das strafrechtliche Haftungsrisiko sind erheblich. Da auch der beste Sprachmittler nicht in der Lage ist, sensible von nicht sensiblen Informationen zweifelsfrei zu unterscheiden, und um der Regelungskomplexität möglichst pragmatisch Herr zu werden, sollte jeder Sprachmittler alle Daten, Informationen und Unterlagen seiner Kunden topsecret behandeln.

Am besten also, man macht keinen Unterschied zwischen Datenschutz und Geheimnisschutz, zwischen personenbezogenen oder nicht personenbezogenen Daten, zwischen Sozialdaten, Fernmeldedaten, Postdaten, besonders sensiblen Daten, Daten über juristische Personen, automatischer oder nicht automatischer Verarbeitung, Erheben, Verarbeiten oder Nutzen, Berufsgeheimnissen, Geschäfts- und Betriebsgeheimnissen, Steuer- und Bankgeheimnis und … und … und. Sondern sorgt mit Verschwiegenheit, Achtsamkeit und einem eigenen technischen Schutzstandard dafür, dass die Sicherheit für alle Daten auf dem Rechner, im Büro und unterwegs gewährleistet ist.

Was tun bei Datenklau oder Datenverlust?

Falls Ihnen ein Laptop oder Speicherstick abhanden kommt oder wenn Sie elektronisch oder auf Papier gespeicherte Daten verlieren und Dritte von diesen unrechtmäßig Kenntnis erlangen oder erlangen können, kann Sie nach § 42a BDSG eine besondere Informationspflicht treffen. Handelt es sich bei den verlorenen Daten um

- besondere Arten personenbezogener Daten (Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen (z. B. der ärztlichen Schweigepflicht),
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen,
- personenbezogene Daten zu Bank- oder Kreditkartenkonten und drohen
- schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen,

müssen Sie den Verlust unverzüglich der für Sie zuständigen Datenschutz-Aufsichtsbehörde sowie den Betroffenen mitteilen. Zum Umfang der Mitteilungspflicht sei auf den genannten Paragraphen verwiesen.
Da eine mangelnde, fehlerhafte, unvollständige oder verspätete Mitteilung empfindliche Bußgelder nach sich ziehen kann, ist Vorsicht bei der Auslegung des „Drohens von schwerwiegenden Beeinträchtigungen" geboten. Sie sind auf der sicheren Seite, wenn die Daten immer wirksam verschlüsselt sind. Dann kann eine Mitteilung an die Betroffenen oder an die Aufsichtsbehörde unterbleiben.

Manuel Cebulla

Diplom-Wirtschaftsjurist, Master of Laws, staatlich geprüfter Übersetzer, geprüfter Datenschutzbeauftragter; Gutachter und Berater für Datenschutz, Mitglied im BDÜ.
m@cebulla-net.de

0404_Datenschutz_Uebersetzer.indd 14 31.08.2011 10:16:20 Uhr