



KEINE CHANCE DEN

DATENDIEBEN

Ein Leitfaden zum Umgang mit vertraulichen Daten



Weitere Informationen zu Fellowes Aktenvernichtern erhalten Sie bei:

Über Fellowes

Fellowes gehört zu den führenden Anbietern von Büromaschinen und Technologiezubehör für den privaten sowie den Office Bereich. Das amerikanische Familienunternehmen mit europäischen Niederlassungen u.a. in Deutschland, Frankreich, Großbritannien und Benelux beschäftigt über 1200 Mitarbeiter weltweit.



I	Sorglosigkeit mit fatalen Folgen	3
II	Betrugsdelikte	6
III	Bin Raiding Studie: Geheimnisse im Altpapier	8
IV	Umgang mit vertraulichen Daten in deutschen Unternehmen	9
V	Wie kann ich mich schützen? Als Privatperson Als Unternehmen	10
VI	Die Gesetzeslage in Deutschland, Österreich, Schweiz	12
VII	Aufbewahrungsfristen	14
VIII	Was können Sie tun, wenn Sie Opfer von Datenmissbrauch werden?	16
IX	7 Regeln zum Schutz persönlicher Daten	17
X	Wie finde ich den passenden Aktenvernichter für meine Bedürfnisse?	18

Sorglosigkeit mit fatalen Folgen

Weiß vielleicht jemand mehr über Sie, als Ihnen lieb ist?

Datenschutz und –missbrauch sowie die sichere Vernichtung persönlicher und vertraulicher Daten sind brisante Themen, die uns sowohl beruflich als auch privat zunehmend betreffen. Doch nur die wenigsten sind sich der Gefahr, Opfer eines Betrugsdeliktes zu werden, bewusst, wie die Ergebnisse einer im Auftrag von Fellowes durchgeführten Bin Raiding Studie* zeigen. Im Altpapier von 1.135 Privat- und 869 gewerblichen Haushalten, wurden sage und schreibe 4.311 Dokumente mit Namens- und Adressdaten gefunden. Privathaushalte, Unternehmen und deren Kunden waren dabei in ungefähr gleichem Maße betroffen. In Einzelfällen wurden ganze Listen mit Kundendaten entsorgt. Bemerkenswert ist auch, dass einzelne Arztpraxen vollständige Patientenakten sorglos wegwarfen.

Egal, ob es sich um Menschen mit krimineller Energie oder solche mit einem speziellen Sinn für Humor handelt: Gelangen persönliche Informationen in falsche Hände, kann dies für Betroffene nicht nur Ärger, sondern auch erhebliche finanzielle Schäden bedeuten.

Vor allem Unternehmen öffnen Betrügern Tür und Tor, wenn sie ihre Aufgabe im Datenschutzbereich nicht ernst nehmen, da sie im Allgemeinen über mehr vertrauliche Daten verfügen als Einzelpersonen. Unternehmen riskieren nicht nur finanzielle Einbußen, sondern setzen auch ihren guten Ruf und das Vertrauen ihrer Kunden aufs Spiel.

Viele müssen sich der Gefahren erst noch bewusst werden. Grundsätzlich gilt:

Vernichten Sie alle Daten, die Sie nicht in den Händen von Fremden sehen wollen!

*Unter Bin Raiding versteht man das systematische Durchsuchen von Hausmüll nach "wertbaren" Informationen wie persönlichen Daten, Bankunterlagen und personalisierten Dokumenten.

Sorglosigkeit mit fatalen Folgen – ein Fallbeispiel

Es klingt fast unglaublich, aber dieser Fall ist leider bittere Realität...

Christian*, 23 Jahre alt, studiert seit zwei Jahren in Passau. Direkt nach dem Umzug in die neue Stadt eröffnete er ein Konto bei der Sparkasse. Die Kreditkarte, die er zu Studentenkonditionen erhalten hat, nutzt er beim Einkaufen, Tanken oder für Bestellungen im Internet. Die Quittungen sammelt er in seinem Geldbeutel und sortiert ältere Belege regelmäßig aus – diese wandern dann direkt in die Mülltonne.

Im Juli erhält er ein Schreiben der Bank, dass er seinen Kreditrahmen überschritten habe. Er wundert sich zwar, aber da er gerade im Prüfungsstress ist, beschließt er, sich direkt nach den Prüfungen dort zu melden. Als jedoch am nächsten Tag beim Tanken seine Kreditkarte abgelehnt wird, geht er doch sofort in seine Filiale, um die Sache zu klären. Dort erfährt er, dass seine beiden Konten überzogen seien. Er hat jedoch nur ein Konto bei der Sparkasse! Der Berater erklärt ihm, dass er doch erst vor sechs Wochen ein zweites Konto eröffnet habe, das bereits mit 2.000 Euro im Minus sei. Letzte Woche habe er sein Guthaben vom ersten Konto auf das Zusatzkonto übertragen und zwei Tage später abgeboben. Christian lässt sich den Antrag für das neue Konto zeigen, der auf seinen Namen, seine Adresse und sogar sein Geburtsdatum ausgestellt ist. Die Unterschrift ist seiner sehr ähnlich, aber er war am Tag der Antragsstellung bei seiner Familie in Nürnberg. Bei der Überprüfung der Kontobewegungen stellt Christian mit Schrecken fest, dass seit der letzten Abrechnung knapp 2.500 Euro mit seiner Kreditkarte bezahlt wurden – und er deshalb beim Tanken nicht damit bezahlen konnte. Er lässt sofort beide Konten und die Kreditkarte sperren. Der Bankberater rät ihm außerdem, alle Unregelmäßigkeiten auf seinem Konto genau zu dokumentieren. Von der Bank geht er direkt zur Polizei, denn er muss Anzeige gegen Unbekannt wegen Identitätsdiebstahl erstatten.

Seither sind vier Wochen vergangen, in denen Christian versucht hat, zu verstehen, wie dies passieren konnte und seine Kreditwürdigkeit wieder herzustellen. Das ist mit viel Ärger, Behördengängen und Papierkram verbunden, denn er ist inzwischen sogar bei der Schufa gelistet. Er hat von den Experten des Betrugsdezernats erfahren, dass oft schon der Name, die Kartenummer und die Gültigkeitsdauer, die alle auf den Kreditkartenbelegen vermerkt sind, ausreichen, um auf den Namen einer anderen Person Bestellungen im Internet vorzunehmen – und schwört sich, in Zukunft keine persönlichen Unterlagen mehr in den Hausmüll zu werfen.

* Name wurde geändert



Sorglosigkeit mit fatalen Folgen – Hinweise für Unternehmen

Ob Banken, Handel, Gesundheitswesen oder IT-Sektor...

der Umgang mit personenbezogenen Daten gehört inzwischen in nahezu jedem Unternehmen zum Arbeitsalltag. Die technische Entwicklung, der Trend zu personalisierten Marketingmaßnahmen und die zunehmende Zahl an Kundenkarten haben ihr Übriges zur Fülle an sensiblen Daten in deutschen Unternehmen beigetragen.



Deshalb ist es heute wichtiger denn je, alle Mitarbeiter für das Thema Datenschutz zu sensibilisieren, insbesondere in Anbetracht der **verschärften gesetzlichen Vorschriften und drohenden Bußgelder**. Fälle wie der eines deutschen Kreditinstituts, dessen Mitarbeiter Lastschriftinformationen mit den kompletten Bankverbindungsdaten ihrer Kunden direkt in die Mülltonne entsorgten, gehen nach der neuen EU-Richtlinie nicht mehr so glimpflich für das entsprechende Unternehmen aus.

Sorglosigkeit mit fatalen Folgen – Hinweise für Unternehmen

Die neue Gesetzgebung gilt jedoch nicht nur für Großunternehmen: Auch kleine und mittlere Unternehmen sind seit dem 23. Mai 2004 mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) **zur Einhaltung konkreter Datenschutzregelungen verpflichtet**. So sind alle Unternehmen, in denen mehr als vier Personen mit sensiblen Daten zu tun haben, verpflichtet, einen Datenschutzbeauftragten zu ernennen. Dieser vertritt die Datenschutzbehörde im Unternehmen und fungiert als interne Kontrollinstanz. Datenschutz muss jedoch nicht nur als eine Bedrohung für Unternehmen verstanden werden, sondern kann auch einen **Wettbewerbsvorteil** darstellen. Richtig kommuniziert können die Datenschutzmaßnahmen eines Unternehmens als Verkaufsargument gegenüber Kunden dienen – insbesondere angesichts der gestiegenen Angst der Verbraucher, die längst den Überblick darüber verloren haben, wie Unternehmen mit ihren persönlichen Daten umgehen.

Betrugsdelikte

Kreditkartenbetrug

Kreditkartenbetrug ist vermutlich das bekannteste Betrugsdelikt. Schon allein mit der Kreditkartennummer, der Gültigkeitsdauer und dem Namen einer Person kann ein Betrüger über das Internet bestellen und so erheblichen Schaden bzw. Unannehmlichkeiten für das Opfer verursachen. Solche Bestellungen aufzuklären und wieder rückgängig zu machen, ist oft schwierig und zeitaufwendig.

Betrug mit Krankenkassenkarten

Neben Kreditkartendelikten nimmt auch der Betrug mit den Chipkarten der Krankenkassen rapide zu. Die Karten enthalten zur Identifikation der versicherten Person lediglich den Namen und das Alter. Da kein Lichtbild vorhanden ist, kann jede Person, die ungefähr den Angaben auf der Chipkarte entspricht – gleiches Geschlecht und ähnliches Alter genügt – die Karte nutzen. Inzwischen sind Fälle bekannt, bei denen eine Karte bis zu 36 Mal pro Quartal eingesetzt wurde. Schätzungen zufolge beläuft sich der Schaden, der deutschen Krankenkassen durch diese Betrugsdelikte entsteht, auf bis zu 50 Prozent des jährlichen Kassendefizits.



Bin Raiding

Unter Bin Raiding versteht man das systematische Durchsuchen von Hausmüll nach „verwertbaren“ Informationen wie persönliche Daten, Bankunterlagen oder personalisierte Dokumente. Eine Studie von Experian in Zusammenarbeit mit der Kriminalpolizei in Großbritannien hat ergeben, dass sich in jeder fünften Mülltonne brisante Informationen befinden, die es Betrügern ermöglichen, persönliche Daten zu missbrauchen.

In den Ballungszentren liegt die Quote sogar bei 40 Prozent.

Betrug am Unternehmen

„Betrug am Unternehmen“ liegt vor, wenn Betrüger die Identität eines Unternehmens nutzen, um Produkte, Dienstleistungen oder finanzielle Mittel zu erwerben. Dies kann die Kreditwürdigkeit des Unternehmens belasten, zu ernsthafter Rufschädigung und letztendlich sogar zum Konkurs führen. Unternehmen haften im Gegensatz zu Privatpersonen für den fahrlässigen Umgang mit vertraulichen Daten. Die nicht ordnungsgemäße Vernichtung von vertraulichen oder sensiblen Daten kann für ein Unternehmen somit schwerwiegende Folgen haben.

Identitätsdiebstahl

Identitätsdiebstahl (englisch: Identity Theft) ist juristisch als „die missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte“ definiert. Dabei werden persönliche Daten wie Geburtsdatum, Anschrift, Sozialversicherungsnummer, Bankkonto oder Kreditkartennummern entwendet, um eine rechtsverbindliche Identitätsfeststellung zu umgehen oder zu verfälschen. Dies kann für die Betroffenen schwerwiegende Folgen wie hohe Schulden oder Anzeigen wegen krimineller Handlungen, die im Namen der entsprechenden Person durchgeführt wurden, zur Folge haben. Am häufigsten tritt Identitätsdiebstahl in Form von Kreditkartenbetrug, Kontenraub oder Bankbetrug auf. In den hochtechnisierten Ländern ist Identitätsdiebstahl eine der am stärksten wachsenden Kriminalitätsformen, die insbesondere durch den E- Commerce seine Plattform gefunden hat.



Bin Raiding Studie: Geheimnisse im Altpapier

Im Rahmen einer im September 2006 im Auftrag von Fellowes durchgeführten Bin Raiding Studie* in einer deutschen Großstadt wurde das Altpapier von über 2000 privaten und gewerblichen Haushalten untersucht. Dabei wurden beunruhigend viele vertrauliche Dokumente entdeckt, mit denen Betrüger bequem in die Identität einer fremden Person schlüpfen könnten:

- 4.311** Dokumente mit Namens- und Adressdaten
- 897** Unterschriften, davon über 50% aus Unternehmen
- 540** Kontoauszüge, die meisten davon im Papiermüll von Privathaushalten
- 156** Kreditkartenbelege

Diese und weitere Fundstücke machen deutlich, dass Unternehmen und Privatpersonen nicht verantwortungsvoll mit ihren personenbezogenen Daten umgehen und Gesetze wie das Bundesdatenschutzgesetz nicht den erhofften Nutzen hinsichtlich des Datenschutzes erbringen.

* Die Studie wurde durchgeführt in Zusammenarbeit mit der Wirtschafts- und Verhaltenswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg.

Umgang mit vertraulichen Daten in deutschen Unternehmen – Ergebnisse einer Umfrage

Im Frühjahr 2005 wurden im Auftrag von Fellowes Geschäftsführer und Manager aus 1005 deutschen Unternehmen folgender Branchen mit erhöhtem Aufkommen an sensiblen Daten befragt: Versicherungswesen, Banken und kleinere Finanzdienstleistungsunternehmen, Gesundheitswesen, Rechtswesen, kleine und mittelständische Unternehmen verschiedener Branchen und Mitarbeiter in Klein- und Heimbüros verschiedener Branchen.

Die Ergebnisse waren teilweise alarmierend:

Von allen befragten Unternehmen haben

49% keine oder nur informelle Richtlinien zur Vernichtung vertraulicher Daten und 46% noch nie von Identitätsdiebstahl gehört.

46%
der Befragten
haben noch nie von
Identitätsdiebstahl
gehört

Im Personalbereich werden

zu 19% Vertragsentwürfe, zu 16% Gehaltsinformationen und zu 15% Personalakten unvernichtet in den Papierkorb geworfen.

In den befragten Banken werden

16% der vertraulichen Daten und 13% aller Dokumente mit Details zu finanziellen Transaktionen in den Papierkorb entsorgt, anstatt vernichtet zu werden .

16%
der befragten
Banken vernichten
vertrauliche Daten nicht

Wie kann ich mich schützen?

Egal ob im Arbeitsalltag oder im Privatleben – bereits mit geringem Aufwand können Sie sich wirkungsvoll gegen Datenmissbrauch schützen. Eine wichtige Grundregel lautet: Archivieren Sie Dokumente, die Sie behalten möchten, vernichten Sie solche, die Sie nicht mehr benötigen.

Privatpersonen

Welche Dokumente sollten Privatpersonen vernichten, wenn sie nicht mehr benötigt werden?

- Verträge
- Rechnungen und Quittungen
- Ausweise
- Medizinische Unterlagen
- Bestellungen
- Kontoauszüge
- Kreditanträge
- Nebenkostenabrechnungen
- Steuerbescheide/ Steuererklärungen
- Personalisierte Werbung
- Adressaufkleber auf abonnierten Zeitungen und Magazinen
- Dokumente mit Ihrer Unterschrift
- Dokumente mit Ihrer Sozialversicherungsnummer



RISKANT



SICHER

Unternehmen

Welche Dokumente sollten Unternehmen vernichten, wenn sie nicht mehr benötigt werden?

- Verträge aller Art
- Rechnungen und Quittungen
- Rechtliche Dokumente
- Steuerliche Unterlagen
- Buchhaltungsunterlagen/ Geschäftsbücher/ Jahresabschlüsse
- Dokumente mit persönlichen Unterschriften
- Daten aus Forschung & Entwicklung
- Personalunterlagen/ Bewerbungsunterlagen
- Business Pläne
- Marketingpläne
- Vertriebsdaten
- Kundenlisten
- Vertrauliche Kundendaten
- Patentinformationen

Tipp:

Auch CDs können vertrauliche Informationen enthalten!



Gesetzeslage in Deutschland, Österreich, Schweiz

In den vergangenen Jahren hat die Legislative auf die steigende Zahl an Datenmissbrauchsfällen reagiert und die Gesetze weiter verschärft. So wurde 1995 eine neue umfassende EU-Datenschutz-Richtlinie verabschiedet, die seit Juni 2004 auch in Deutschland in Kraft getreten ist. Verstöße gegen dieses Gesetz können mit Bußgeldern von bis zu 250.000 Euro und gegebenenfalls sogar mit Freiheitsstrafen geahndet werden.

Die Europäische Datenschutzrichtlinie

Mit der Europäischen Datenschutzrichtlinie vom 24.10.1995 trägt die EU dem Schutz der Privatsphäre in der Informations- und Kommunikationsgesellschaft Rechnung. Damit wurde das bislang von den Mitgliedsstaaten unterschiedlich geregelte Datenschutzrecht auf einer modernen Grundlage europaweit harmonisiert und weiter ausgebaut. So ist zum Beispiel der Datenschutz in der Europäischen Grundrechtscharta und im Europäischen Informationszugangsgesetz verankert und die praktische Zusammenarbeit der Datenschutz-Kontrollinstanzen in Artikel 29 der Datenschutzrichtlinie geregelt.

Gesetzeslage zum Datenschutz in Deutschland

In Deutschland findet sich die Grundlage für ein Sicherheitskonzept in der Anlage zu § 9 S.1 des Bundesdatenschutzgesetzes (BDSG): Der Katalog von technischen und organisatorischen Maßnahmen gewährleistet ein angemessenes Datensicherheitsniveau. Entsprechende Regelungen sind in den Landesdatenschutzgesetzen festgelegt. Diese Normen definieren zwar keine konkreten Kriterien, geben jedoch Zielvorgaben für den Gesamtkomplex der Datensicherheit, welche bei der Erarbeitung von Sicherheitskonzepten Berücksichtigung finden sollen.

Datenschutz in Unternehmen

Personenbezogene Daten werden in Wirtschaftsunternehmen für unterschiedlichste Zwecke benötigt: Von der Personaldatenverarbeitung, der Kundenbetreuung bis hin zur Auswertung von Informationen über Interessenten an Produkten und Dienstleistungen. Daher existieren zahlreiche gesetzliche Vorschriften, die den Umgang mit personenbezogenen Daten durch Wirtschaftsunternehmen regeln. Zumeist gibt das BDSG, insbesondere seine §§ 1 ff. und 27 ff., den Rahmen der zulässigen Datenverarbeitung vor.

Datenschutzbeauftragte in deutschen Unternehmen

Nach § 4ff des BDSG besteht die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen, für alle Unternehmen, in denen mehr als neun Personen mit sensiblen Daten wie Kunden- oder Personaldaten zu tun haben. Der Datenschutzbeauftragte dient als interne Selbstkontrollinstanz, die die Datenschutzbehörde im Unternehmen vertritt. Das Gesetz gilt neben Unternehmen auch für Organisationen und Vereine. Das Nichteinberufen eines Datenschutzbeauftragten kann mit bis zu 25.000 Euro Bußgeld geahndet werden.

Datenschutzkontrolle

In Deutschland sind unterschiedliche Kontrollinstanzen tätig. Im öffentlichen Bereich, vor allem bei den Behörden, sorgen die Landesbeauftragten oder der Bundesbeauftragte für den Datenschutz für die Einhaltung der Vorschriften. Im privaten Sektor übernehmen die Aufsichtsbehörden nach § 38 BDSG diese Aufgabe, wobei es die einzelnen Bundesländer unterschiedlich regeln, welche Behörde tätig wird.

Gesetzeslage zum Datenschutz in Österreich

Das Verständnis von Datenschutz in Österreich basiert auf dem Anspruch eines jeden Bürgers auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse – insbesondere im Hinblick auf sein Privat- und Familienleben – besteht.

Die rechtliche Grundlage bildet das Datenschutzgesetz 2000 (DSG), in dem das „Grundrecht auf Datenschutz“ (§1) als Verfassungsbestimmung festgelegt ist. Darüber hinaus gibt es ergänzende Normen, wie z.B. die ÖNORM S 2109 „Akten- und Datenvernichtung“, die eine Definition der Schutzbedürftigkeit sensiblen Datenmaterials festlegt und im Detail erläutert, unter welchen Bedingungen Daten aus Papier als sicher vernichtet gelten. Als Kontrollinstanzen sorgen die Datenschutzkommission, eine gerichtsähnliche Verwaltungsbehörde, und der Datenschutzrat, der die Entwicklung verfolgt und Empfehlungen abgibt, für die Einhaltung und Weiterentwicklung des Datenschutzgesetzes in Österreich. Weitere Informationen finden Interessierte auf der Website der Datenschutzkommission Österreich unter www.dsk.gv.at.

Gesetzeslage zum Datenschutz in der Schweiz

Gesetzlich verankert ist das Thema Datenschutz im Bundesgesetz über den Datenschutz (DSG) aus dem Jahr 1992 und in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) aus dem Jahr 1993. Das DSG regelt unter anderem das „Bearbeiten von Personendaten durch private Personen“ und das „Bearbeiten von Personendaten durch Bundesorgane“. Ein separater Abschnitt befasst sich mit der Rolle des eidgenössischen Datenschutzbeauftragten, der die Einhaltung des Gesetzes durch die Bundesorgane überwacht und private Personen in Sachen Datenschutz berät. Ein letzter Abschnitt regelt die Strafbestimmungen, denen zufolge Verstöße gegen das DSG mit Bußgeldern und sogar Haft geahndet werden können. Neben dem eidgenössischen Datenschutzbeauftragten auf Bundesebene, gibt es auf Ebene der einzelnen Kantone Datenschutzbehörden, die sich um regionale Belange kümmern. www.edsb.ch.

Aufbewahrungsfristen

Empfehlungen zu Aufbewahrungsfristen von Dokumenten

Vorschriften zu Aufbewahrungsfristen von Dokumenten finden sich in verschiedenen Gesetzestexten, wie beispielsweise im Handelsgesetzbuch (HGB), im Steuerrecht (EStG, KStG, GewStG, AO) und im Zivilrecht (BGB, ZPO). Grundsätzlich gelten für digitale und Papierunterlagen dieselben Regeln für die Aufbewahrung: Die Frist beginnt jeweils mit dem Ende des Kalenderjahres, in dem letzte Änderungen in den Dokumenten vorgenommen wurden.

Wichtige Hinweise für Unternehmen:

Jeder Kaufmann ist verpflichtet, geschäftliche Unterlagen über einen gewissen Zeitraum aufzubewahren. Man unterscheidet dabei zwischen Fristen von sechs Jahren und Fristen von zehn Jahren.

10 Jahre:

- Eröffnungsbilanzen
- Buchungsunterlagen und -belege, Handelsbücher
- Inventuren
- Jahresabschlüsse (in Papierform!)
- Konzernabschlüsse und -lageberichte
- Projektunterlagen, Arbeitsanweisungen
- Lohnsteuerunterlagen



6 Jahre:

- Empfangene und verschickte Korrespondenz zu jeglichen Geschäftsvorfällen (z. B. Bestellungen, Bestätigungen, Rechnungen)
- Weitere, für die Besteuerung relevante, Unterlagen

Darüber hinaus empfiehlt sich für Bankauszüge, Zahlungsbelege und Kreditunterlagen in der Praxis eine Aufbewahrungsfrist von 30 Jahren, da diese der Gewährungsfrist der Banken entspricht.

Wichtige Hinweise für Privatpersonen:

Für Privatpersonen unterscheidet man Dokumente, die lebenslang aufbewahrt werden sollten und Unterlagen, die bis Vertragsende bzw. Verkauf verwahrt werden sollten.

Lebenslang:

- Geburtsurkunde / Taufschein
- Heiratsurkunde
- Zeugnisse / Ausbildungsurkunden
- Sterbeurkunden von Familienangehörigen
- Ärztliche Gutachten
- Unterlagen zur Rentenberechnung (Arbeitsverträge, jährliche Sozialversicherungsnachweise, Gehaltsabrechnungen)

Bis Vertragsende bzw. Verkauf:

- Wohnmiete (Mietvertrag, Übergabeprotokoll, Nebenkostenabrechnung)
- Wohneigentum (Grundbuchauszug, Baurechnungen, Bauzeichnungen)
- Versicherungspolicen

Allgemeine Aufbewahrungsfristen:

Einige Aufbewahrungsfristen treffen für Unternehmen und Privatpersonen gleichermaßen zu.

6 Monate:

- Handwerksleistungen (schriftliche Gewährleistungen)
- Quittungen (Anspruch auf Mängelbeseitigung 6 Monate nach Kauf)
- Reismängel (Reklamation bis 6 Monate nach Urlaubsende)

2 Jahre:

- Kaufverträge
- Rechnungen von Ärzten, Anwälten, Notaren

10 Jahre:

- Komplette Unterlagen zur Steuererklärung

30 Jahre:

- Urteile, Mahnbescheide, Prozessakten

Was können Sie tun, wenn Sie Opfer von Datenmissbrauch werden?

- 1 Kontaktieren Sie umgehend Ihre Bank oder Ihr Kreditkartenunternehmen und lassen Sie Ihre Konten und Karten sperren.
- 2 Wenden Sie sich an die nächste Polizeidienststelle und melden Sie den Betrug.
- 3 Informieren Sie Ihre Bankniederlassung bzw. Ihren Bankberater über den Betrugsfall.
- 4 Dokumentieren und protokollieren Sie alle das Betrugsdelikt betreffenden Aktivitäten, Gespräche und Telefonate. Dies erleichtert im Zweifelsfall eine Rückverfolgung.

Darüber hinaus, gibt es eine Reihe Experten, an die Sie sich wenden können, wenn Sie Hilfestellung benötigen.

Hier einige nützliche Kontaktadressen:

Deutschland:

Das virtuelle Datenschutzbüro – zentrale Informations- und Anlaufstelle sämtlicher Datenschutzinstitutionen: <http://www.datenschutz.de>
Berufsgruppe der Datenschutzbeauftragten: <http://www.bvdnet.de>
Gesellschaft für Datenschutz und Datensicherheit (GDD): <http://www.gdd.de>
Kriminalpolizeiliche Beratungsstellen: <http://www.polizei.prpk.de>
Verbraucherzentrale je Bundesland: <http://www.verbraucherzentrale.de>
Online-Anwalts-Beratungsforum: <http://www.expertenzentrale.de>
Direkte telefonische Anwaltsberatung: <http://www.deutsche-anwalts hotline.de>

Österreich:

Datenschutzkommission für Österreich: <http://www.dsk.gv.at>

Schweiz:

Eidgenössischer Datenschutzbeauftragter: <http://www.edsb.ch>
Datenschutzbeauftragter des Kantons Zürich: <http://www.datenschutz.ch>

7 Regeln zum Schutz persönlicher Daten

- 1 Nutzen Sie einen Aktenvernichter, um Ihre persönlichen Unterlagen zu vernichten und werfen Sie keine Papierunterlagen, die persönliche Daten in jeglicher Art enthalten, in lesbarer Form in den Papierkorb.
- 2 Schaffen Sie sich ein Ablage- bzw. Ordnungssystem, so dass Sie ohne großen Aufwand sämtliche persönlichen Unterlagen sicher aufbewahren und vor unbefugtem Zugriff schützen können.
- 3 Lassen Sie Unterlagen, aus denen persönliche Daten ersichtlich sind, nicht offen liegen: weder im Auto, noch lose in Ihrer Tasche oder in Gegenwart Dritter. Selbst Zuhause sollten persönliche Unterlagen sicher verwahrt werden.
- 4 Achten Sie darauf, dass keine Postsendung aus Ihrem Briefkastenschlitz ragt und dadurch von Fremden entwendet werden kann. Auch Sendungen und Zeitschriften, die häufig von den Boten im Hausflur abgelegt werden, sollten nicht über längere Zeit liegen bleiben.
- 5 Nehmen Sie bei Kartenzahlungen stets die Belege mit, auch wenn Sie sie nicht weiter benötigen – sie enthalten Ihre vollständigen Kontodaten!
- 6 Achten Sie bewusst darauf, welche Unterlagen persönliche Daten enthalten; entwickeln Sie einen Blick dafür, unter welchen Umständen Ihre persönlichen Daten dem Zugriff durch andere ausgesetzt sind.
- 7 Erstellen Sie eine Liste mit Adressen, Kontaktpersonen und Telefonnummern sowie Kunden- oder Vertragsnummern für alle Behörden oder Institutionen, mit denen Sie zu tun haben. So können Sie ohne langes Suchen nach Telefonnummern handeln, wenn Ihnen wichtige Unterlagen abhanden gekommen sind oder Sie vermuten, dass ein Dritter in Ihrem Namen agiert. Beste Beispiele hierfür sind der Verlust der EC- oder Kreditkarte oder unerklärliche Abbuchungen von Ihrem Konto. Halten Sie daher die Servicenummern für eine Sperrung der Karten griffbereit.

Wie finde ich den passenden Aktenvernichter für meine Bedürfnisse?

Beim Erwerb eines Aktenvernichters sollten Sie das Einsatzgebiet sowie die Sicherheitsanforderungen berücksichtigen und die besonderen Produktmerkmale der verschiedenen Geräte kennen. Um sicher zu stellen, dass Sie den richtigen Aktenvernichter für Ihre Anforderungen wählen, beantworten Sie folgende Fragen:

Wie viele Personen werden den Aktenvernichter benutzen?

Persönliche Aktenvernichter:

...Konzipiert für den persönlichen Gebrauch Zuhause, im Heimbüro oder am Arbeitsplatz im Unternehmen

Büro-Aktenvernichter:

...Konzipiert für den Dauerbetrieb durch mehrere Benutzer in Klein - und Großbüros

Welche Sicherheitsanforderungen haben Sie?



Aktenvernichter mit Cross Cut (Partikelschnitt) bieten den höchsten Sicherheitsstandard, da sie das Papier in konfettiähnliche Teilchen zerkleinern. Darüber hinaus reduzieren Sie das Papierabfallvolumen auf bis zu ein Fünftel.



Aktenvernichter mit Streifenschnitt genügen alltäglichen Sicherheitsansprüchen durch Zerkleinerung des Papiers in unleserliche Streifen.

Die Sicherheitsstufen für Aktenvernichtung im Einzelnen:

- Sicherheitsstufe 1:** Streifenschnitt 10,5 mm / Partikelschnitt 10,5 x 40 - 80 mm. Schriftstücke werden zwar schnell unleserlich gemacht, Profis können diese jedoch wieder zusammensetzen.
- Sicherheitsstufe 2:** Streifenschnitt 3,9 oder 5,8mm / Partikelschnitt 7,5 x 40 - 80 mm. Auch Dokumente, die auf dieser Stufe vernichtet werden, sind noch rekonstruierbar und daher sicherheitstechnisch nicht ganz unbedenklich.
- Sicherheitsstufe 3:** Streifenschnitt 1,9 mm / Partikelschnitt 3,9 x 30 - 50 mm. Auf dieser Stufe ist ein Sicherheitsniveau erreicht, das bereits für die Vernichtung vertraulicher oder nur zum internen Gebrauch freigegeben er Daten geeignet ist.
- Sicherheitsstufe 4:** Partikelschnitt 1,9 x 15 mm. Diese Stufe bietet bereits höchste Sicherheit.
- Sicherheitsstufe 5:** Partikelschnitt 0,78 x 11 mm. Hier ist bereits das Sicherheitsniveau von Geheimdiensten erreicht.

Kleinere Stücke, Größere Sicherheit.

Die neuen **Microshred** Aktenvernichter MS-450Cs und MS-460Cs zerkleinern Papier in winzige Partikel, kleiner noch als eine Heftklammer, und vernichten auch Kreditkarten, Büoklammern und CDs mit Leichtigkeit. Sie schützen Unternehmen gegen Datendiebe und dank der neuen **Safe Sense™** Technologie schützen sie auch den Anwender. **Ultra leise. Ultra sicher.**



www.fellowes.eu

THE WORLD'S TOUGHEST SHREDDERS™  Fellowes

