Thema:
Datenschutzsensibilisierung der Mitarbeiter/innen / LSB plus Töchter

(Interne Informationsschrift des LSB von Wolfram Fähnrich, Betrieblicher Datenschutzbeauftragter wolfram.faehnrich@lsb-nrw.de)

Einleitung

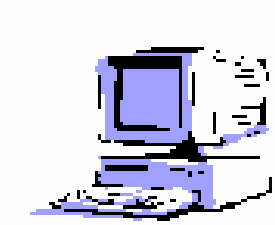
Der Begriff "Datenschutz" ist zwar ein Wort unserer Zeit, aber die Vertraulichkeit der Informationen ist seit jeher ein Bestandteil der menschlichen Umgangsformen. Man denke vor allem an das Schweigegelübde der Ärzte (nachweisbar seit ca. 800 vor Christi Geburt), das Beichtgeheimnis und besondere Berufsgeheimnisse bei Rechtsanwälten und Steuerberatern oder an die Vertraulichkeitsgrundsätze, die die Rechtsprechung für das Personalwesen entwickelt hat.

Mit den modernen informationstechnischen Möglichkeiten erkannte man in den siebziger Jahren die Notwendigkeit, die Verarbeitung von personenbezogenen Daten zu regeln. Der Gesetzgeber wollte den "gläsernen Menschen" verhindern. Als Antwort auf die Risiken der modernen Informationstechnologien für das Persönlichkeitsrecht wurden in Deutschland das Bundesdatenschutzgesetz (BDSG) und andere Datenschutzvorschriften zu bereichsspezifischem Datenschutz geschaffen.

Jeder Bürger hat ein Recht darauf zu wissen, wer welche Daten über ihn zu welchem Zweck wo speichert, verarbeitet und nutzt. Diesen Grundsatz hat das Bundesverfassungsgericht 1983 als "Recht auf informationelle Selbstbestimmung" bezeichnet.

Datenschutz soll dem Bürger dienen, es ist ein Persönlichkeitsrecht.

Verschiedene Gesetze reglementieren die Verarbeitung von Mitarbeiterdaten, Kundendaten, persönlichen Angaben über Menschen der Zeitgeschichte, Bilder und (digitale) Tonaufnahmen mit dem Ziel, die Persönlichkeitsrechte der betroffenen Menschen zu schützen. Rechtsvorschriften, die ausdrücklich eine Datenverarbeitung verbieten, anordnen oder erlauben, gehen dem Datenschutzgesetz vor.



Insoweit ist das BDSG ein Auffanggesetz, es ist subsidiär, also untergeordnet.

In der betrieblichen Praxis stehen bestimmte Fragestellungen des Datenschutzrechts im Vordergrund, die im folgenden Text erläutert werden. Außerdem stellen bestimmte Arbeitsbereiche, wie beispielsweise das Call Center, die DV-Abteilung und das Personalwesen besondere Anforderungen, über die sie noch ausführlich informiert werden.

Was wird geschützt ?

(.... personenbezogene Angaben bei der automatisierten Verarbeitung und in strukturierten, manuellen Dateien.)

Alle Angaben zu einem Menschen, seien es Namen und Anschrift, Telefonnummern, Vertragsbeziehungen, Angaben zu Vermögensverhältnissen, Verhalten oder Zugehörigkeit zu Gruppen fallen unter die Regelungen des BDSG, wenn diese personenbezogenen Daten bei der automatisierten Verarbeitung oder in strukturierten, manuellen Dateien verarbeitet werden. Die folgenden Datenschutzregelungen gelten für die Erhebung, Verarbeitung und Nutzung dieser Daten.

Angaben über Unternehmen fallen nicht unter den Anwendungsbereich des BDSG. Häufig enthalten Kunden-, Lieferanten- und Marketingdateien aber Angaben zu Kontaktpersonen und deren Hobbys und Vorlieben (Vertriebsmitarbeiter, Kundendienst). Alle Daten über diese Personen sind natürlich vom BDSG geschützt.

Wann dürfen die Daten verarbeitet werden ?
(.... nur wenn das BDSG oder eine andere Rechtsvorschrift die Verarbeitung erlaubt.)

Im BDSG gilt das so genannte Verbotsprinzip. Jede Verarbeitung personenbezogener Daten ist verboten, solange sie nicht per Gesetz erlaubt ist. Im BDSG und in anderen (vorrangigen) Rechtsvorschriften finden sich deshalb Regelungen, die eine Verarbeitung anordnen oder rechtfertigen. Vorrangige Rechtsvorschriften werden meist durch Behörden angewandt, die bestimmte Aussagen vom Bürger oder vom Arbeitgeber über die Arbeitnehmer einfordern (Melderecht, Sozialrecht, Steuerrecht).
Das BDSG erlaubt privaten Stellen (also uns) eine nicht ausschließlich private Nutzung zur Erfüllung eigener Geschäftszwecke, wenn:

- es dem Zweck des Vertrages oder der Vertragsanbahnung mit dem Betroffenen dient.
- eine Einwilligung des Betroffenen vorliegt oder aufgrund seines Verhaltens angenommen werden kann.
- wenn die berechtigten Interessen der verantwortlichen Stelle die schutzwürdigen Interessen des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen.
- die Daten allgemein zugänglich sind oder aufgrund ihres Charakters veröffentlicht werden dürften.

Bei der Erhebung der Daten ist der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.

Welche Pflichten hat das Unternehmen ?

- Prüfung der Zulässigkeit, Erforderlichkeit und Zweckbindung
- Sicherstellung der Rechte der Betroffenen und Datensicherungsmaßnahmen

Das Unternehmen hat für jede Verarbeitung personenbezogener Daten zu prüfen, ob eine ausreichende Rechtsgrundlage vorliegt. Wie bereits erläutert, bieten sich als Rechtsgrundlagen eine vorrangige Rechtsvorschrift, die Vertragsanbahnung oder -beziehung mit einem Betroffenen, eine Güterabwägung (berechtigtes Interesse gegen die schutzwürdigen Belange des Einzelnen) oder seine Einwilligung an. Die erhobenen und gespeicherten Daten müssen für die Erfüllung der Arbeitsaufgabe erforderlich sein. Das ist nur der Fall, wenn ohne ihre Kenntnis das berechtigte Ziel der Datenverarbeitung nicht erreichbar wäre.

Weiterhin dürfen die Daten nur für solche Zwecke verwendet werden, zu denen sie auch erhoben und gespeichert wurden (Zweckbindung), oder wo eine Verträglichkeit zwischen dem ursprünglichen Zweck der Erhebung und dem neuen Zweck bejaht werden kann. Wenn bestehende Datenbanken mit personenbezogenen Daten für völlig neue Zwecke verwendet werden sollen, ist die Planung rechtzeitig mit dem betrieblichen Datenschutzbeauftragten abzustimmen.

Der Betroffene ist nach § 33 BDSG über die erstmalige Speicherung seiner Daten zu benachrichtigen. Von der Informationspflicht gelten aber zahlreiche Ausnahmen. Beispielsweise kann auf die Benachrichtigung verzichtet werden, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung erhält. Dem Betroffenen sind die Rechte auf Auskunft, Berichtigung, Sperrung und Löschung (§§ 34,35 BDSG) seiner personenbezogenen Daten zu gewährleisten. Erfahrungsgemäß sind solche Anfragen von Betroffenen sehr selten. Mit geeigneten und angemessenen Datensicherungsmaßnahmen hat das Unternehmen sicherzustellen, dass die Persönlichkeitsrechte der Betroffenen nicht durch Verlust, Verfälschung oder unbefugte Kenntnisnahme durch Dritte verletzt werden (§ 9 BDSG).
Auch unser Unternehmen (Red.: hier LSB) ist verpflichtet einen betrieblichen Datenschutzbeauftragten zu bestellen. Dazu wurde Herr Wolfram Fähnrich berufen. Er hat unter anderem die gesetzliche Aufgabe, auf die Beachtung und Einhaltung des Datenschutzes hinzuwirken. Für Mitarbeiter, Kunden und Lieferanten steht er jederzeit für Rückfragen und Informationen zur Verfügung.

Welche Pflichten haben die Mitarbeiter ?

- Datenschutz-Information und Verpflichtung auf das Datengeheimnis
- Einhaltung der angeordneten Maßnahmen

Die Mitarbeiter/innen, die personenbezogene Daten erheben, verarbeiten und nutzen haben sich mit den Datenschutzvorschriften vertraut zu machen (siehe Dienstanweisung Datenschutz, die ihnen bereits zugestellt wurde, die Mitarbeiter/innen der Außenstellen werden diese Dienstanweisung noch erhalten) und sind vom Unternehmen auf die Einhaltung des Datengeheimnisses nach § 5 BDSG zu verpflichten. Diese Maßnahme (§ 5) ist beim LandesSportBund NRW e.V. abgeschlossen und konzentriert sich nun auf unser Personal bei den Töchtern (BW - lsb/ JFW - lsb), sowie auf jede Neueinstellung.

Diese Mitarbeiterinformation dient der Mitarbeiteraufklärung, wie sie vom Gesetz im Rahmen der Verpflichtung auf das Datengeheimnis vorgeschrieben wird. Darüber hinaus können sich alle Mitarbeiter für weitergehende Informationen direkt an den betrieblichen Datenschutzbeauftragten wenden. Datenschutz verstehe ich nicht als Massenabfertigung, sondern als Einzelberatung, da jeder Arbeitsplatz eines jeden Einzelnen individuell gestaltet ist.

Durch ihre Tätigkeit und die Einhaltung der betrieblichen Datensicherungsmaßnahmen haben die Mitarbeiter/innen sicherzustellen, dass die ihnen anvertrauten personenbezogenen Daten unberechtigten Dritten nicht zur Kenntnis gelangen und die Daten nicht verfälscht oder vernichtet werden.

Das zugeteilte oder selbst gewählte Passwort muss unbedingt vertraulich verwandt werden und ist Dritten nicht mündlich, durch ungeschickte Aufbewahrung (unter der Tastatur, im Schreibtisch) oder auf andere Weise zur Kenntnis zu geben. Die angeordneten Datensicherungsmaßnahmen (Verschluss; Sicherheitskopien; Verbot des Einsatzes ungenehmigter Datenträger, Hard- und Software; sorgfältiger Umgang mit Geräten, vor allem im mobilen Einsatz (Notebooks)) sind strikt einzuhalten.

Welche Rechte hat der Betroffene (§§ 33 bis 35 BDSG)?

- Benachrichtigung, Auskunft, Berichtigung, Sperrung, Löschung
- Anrufung der Aufsichtsbehörde für den Datenschutz, Schadenersatz

Durch das Unternehmen ist dem Betroffenen die erstmalige Speicherung seiner personenbezogenen Daten mitzuteilen, sofern er nicht auf andere Art und Weise Kenntnis über die Datenspeicherung erlangt. Das ist der Fall, wenn offensichtlich datenverarbeitende Prozesse ein Vertragsverhältnis (Arbeitsvertrag, Kaufvertrag, Liefervertrag) begleiten oder wenn er selbst seine Daten zur Speicherung bekannt gibt (Bewerbung, Couponeinsendung, Anmeldung zu Lehrgängen etc.). Außerdem besteht keine Benachrichtigungspflicht, wenn Daten aus allgemein zugänglichen Quellen (Telefonbuch) entnommen werden können. Sollten Fragen über die Gestaltung der Information an einen Betroffenen bestehen, können nähere Informationen beim betrieblichen Datenschutzbeauftragten angefragt werden.

Der Betroffene kann jederzeit unentgeltlich Auskunft von der verantwortlichen Stelle über alle zu seiner Person in Dateien gespeicherten Daten verlangen. Nur bestimmte Unternehmen, wie beispielsweise Kreditschutzorganisationen und Handels- und Wirtschaftsauskunfteien, können ein Entgelt verlangen. Der Betroffene kann verlangen, dass falsche Daten berichtigt, unberechtigt gespeicherte oder unrichtige Daten gesperrt (der weiteren Verarbeitung entzogen) oder ganz gelöscht werden. Die Sperrung von Daten ist vor allem dann angezeigt, wenn rechtliche Aufbewahrungsvorschriften einer sonst erforderlichen Löschung entgegenstehen. Zuletzt kann sich der Betroffene auch mit einer Beschwerde an die Datenschutzaufsichtsbehörde wenden oder für unzulässige oder falsche Datenverarbeitung Schadenersatz verlangen.

Wer kontrolliert den Datenschutz ?

- betriebliche Selbstkontrolle durch den Datenschutzbeauftragten
- Fremdkontrolle durch Aufsichtsbehörden für den Datenschutz

Der Betroffene muss in der Regel selbst entscheiden, welche seiner Daten er den Vertragspartnern oder der Werbewirtschaft zur Verfügung stellt. Dabei sollte er immer prüfen, ob die angegebenen Daten für die Erfüllung des Vertragszwecks erforderlich sind. Wünscht er keine Werbesendungen, so muss er allen Versuchungen widerstehen, die von Preisausschreiben, Glücksspielen und kostenlosen Probesendungen ausgehen. Zusätzlich kann er sich auch in die "Robinson-Liste" des Deutschen Direktmarketing-Verbandes eintragen lassen, dessen Mitglieder dann Werbe-Mailings an ihn unterlassen.

Der betriebliche Datenschutzbeauftragte des Unternehmens prüft im Rahmen seiner Tätigkeit, ob die in Frage stehenden personenbezogenen Daten zulässig erhoben, für den Vertragszweck erforderlich sind, zweckgebunden eingesetzt und unter angemessenen Sicherheitsvorkehrungen verarbeitet werden, wenn er hierüber rechtzeitig informiert wird.

Der betriebliche Datenschutzbeauftragte berät die Geschäftsführung und die Mitarbeiter/innen und steht bei Fragen zum datenschutzgerechten Umgang mit personenbezogenen Daten zur Verfügung. Er ist eine Einrichtung der "Selbstkontrolle", durch die der Gesetzgeber einer "Datenschutz-Bürokratie" durch staatliche Aufsicht entgegenwirken wollte.

Bei Zweifeln an der Rechtmäßigkeit der Datenverarbeitung in einem Unternehmen kann sich der Betroffene an den betrieblichen Datenschutzbeauftragten oder an die zuständige Aufsichtsbehörde für den Datenschutz wenden. Die Datenschutzaufsichtsbehörden sind, je nach Bundesland, den Innenministerien, Regierungspräsidien oder Staatsministerien des Innern angegliedert. Diese prüfen die Datenverarbeitung in allen privaten Einrichtungen.

Wenn sich die zuständige Aufsichtsbehörde mit einer Anfrage an das Unternehmen wendet, dann ist diese unbedingt an die Geschäftsführung mit einem Antwortentwurf weiterzuleiten. Die Geschäftsführung informiert dann ihrerseits den betrieblichen Datenschutzbeauftragten um die Form und den Inhalt der Antwort datenschutzkonform abzustimmen.

Welche Konsequenzen haben Datenschutzverletzungen?

- Imageverlust für Unternehmen und Mitarbeiter / innen
- Straf- und Bußgelder nach §§ 43, 44 BDSG
- arbeitsrechtliche Konsequenzen
- Schadenersatzpflichten

Die Beachtung der Datenschutzvorschriften kennzeichnet eine ordnungsgemäße Datenverarbeitung und wurde in den letzten Jahren in der Wirtschaft zum Qualitätsmerkmal. Unzulässige Veröffentlichungen von sensiblen Kunden- und Mitarbeiterdaten führen in der Regel zu Imageverlusten. Werden personenbezogene Daten vorsätzlich oder fahrlässig entgegen den Bestimmungen des Datenschutzgesetzes erhoben, verarbeitet, genutzt, Dritten übermittelt, unberechtigterweise verändert oder gelöscht, kann dies eine Geldstrafe bis Euro 250.000,00 oder bis zu zwei Jahren Freiheitsstrafe zur Folge haben.

Werden Auflagen des Datenschutzgesetzes, wie die Benachrichtigung der Betroffenen, die rechtzeitige Bestellung eines Datenschutzbeauftragten und vorgeschriebene Meldungen an die Aufsichtsbehörde nicht, nicht richtig oder nicht rechtzeitig erfüllt, so hat das Unternehmen wegen Ordnungswidrigkeiten mit Bußgeldern von Euro 25.000,00 zu rechnen.

Schadenersatzpflichten entstehen, wenn Rechte des Betroffenen durch unzulässige oder unrichtige Datenverarbeitung verletzt werden. Dabei liegt die Beweislast, dass kein Verschulden des Unternehmens vorliegt, immer beim Unternehmen. Hierbei handelt es sich um die so genannte Beweislastumkehr.

Wenn Mitarbeiter gegen datenschutzrechtlich begründete betriebliche Anweisungen handeln, können auch arbeitsrechtliche Maßnahmen abgeleitet werden.

Beim Bundesdatenschutzgesetz handelt es sich um ein Schutzgesetz und immer dann, wenn Schutzgesetze verletzt werden besteht Anspruch auf Schadenersatz.

Auskunftsersuchen

- Auskünfte an Betroffene über die über sie selbst gespeicherten Daten müssen vollständig, umfassend und richtig sein. Grundsätzlich haben alle Betroffenen das Recht auf Auskunft über die von ihnen gespeicherten personenbezogenen Daten, sei es in automatisierten Verarbeitungen (DV-mäßig) oder in strukturierten manuellen Dateien (systematische Aktensammlungen). Das BDSG nennt einige Ausnahmetatbestände; deshalb sind Auskunftsersuchen von Betroffenen über die Geschäftsführung dem betrieblichen Datenschutzbeauftragten zuzuleiten, mit dem Hinweis, in welchem Bereich welche Daten verarbeitet und in welcher Weise genutzt wurden.
- Auskünfte an öffentliche Stellen sind dann zulässig, wenn die Anfragen aufgrund einer Rechtsvorschrift erfolgen. Die Anfrage von Behörden und öffentlichen Stellen muss unter Angabe der Rechtsgrundlage (Paragraph und Gesetz) und der Nennung des Zwecks des Auskunftsersuchens erfolgen. Alle nicht routinemäßigen Anfragen öffentlicher Stellen, im Telekommunikationsbereich insbesondere der Polizei, sind zur Prüfung an die Geschäftsführung weiterzuleiten.
- Ausländische öffentliche Stellen haben keinen Anspruch auf Auskunft! Die Anfragen sind zur Prüfung an die Geschäftsführung weiterzuleiten.
- Auskunftsanfragen der Presse sind an die Geschäftsführung weiterzuleiten. Eine gute Zusammenarbeit mit der Presse ist für das Unternehmen sehr wichtig. Trotzdem darf nicht jeder Mitarbeiter Auskunft erteilen.
- Auskünfte an sonstige Dritte sind sehr genau zu prüfen; es besteht i.d.R. kein Rechtsanspruch auf Auskunft! Nur in wenigen Ausnahmen dürfen auch Dritte Auskünfte über Personen erhalten. Die Auskunftserteilung sollte restriktiv, also eingeschränkt, gehandhabt und mit der Geschäftsführung abgestimmt werden.
- Telefonische Auskunftsersuchen: Telefonisch dürfen nur dann Auskünfte über personenbezogene Daten erteilt werden, wenn sich zweifelsfrei feststellen lässt, ob der Anrufer auch wirklich derjenige ist, für den er sich ausgibt und ob eine entsprechende Vorschrift die Auskunftserteilung erzwingt oder zulässt. Zweckmäßig ist, wenn bei einer zulässigen Auskunft die anfragende Stelle nach vorheriger Prüfung der mitgeteilten Telefonnummer über ihre Telefonzentrale zurückgerufen wird.

Archivierung / Entsorgung

- Die Aufbewahrung personenbezogener Daten ist nur so lange zulässig, wie es Aufbewahrungsvorschriften zulassen.

Die nach gesetzlichen (hier sind vor allem HGB und Abgabenordnung zu nennen), satzungsgemäßen oder vertraglichen Vorschriften aufzubewahrenden Daten sind entsprechend ihrer Fristen und der notwendigen Sicherheitsstufe zu lagern.

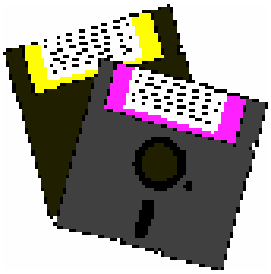
Nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen sind zu vernichtende Papier-Datenträger entweder mittels Aktenvernichter zu vernichten oder gesammelt einem Unternehmen zu übergeben, das als zuverlässiger Auftragsdatenverarbeiter für die Aktenvernichtung gilt.

Das gilt auch für defekte Disketten, Datenbänder oder einmal beschreibbare Karbonbänder. Keinesfalls dürfen personenbezogene (oder auch sonstige sensible firmeninterne) Daten dem Hausmüll zugeführt werden!

Ein softwaremäßiges Löschen von Datenträgern der PC-Technik (Festplatten, Disketten, Bänder) oder die Abgabe von Festplatten zur Reparatur/Gewährleistung ist in der Regel nicht ausreichend, wenn die Daten mit Hilfe von Tools oder anderen Verfahren wieder lesbar gemacht werden können!

Datensicherheit (§ 9 und Anlage zu § 9 BDSG)

- Schutz vor Verlust, Verfälschung, Verfügbarkeitseinschränkung, und Kenntnisnahme durch unberechtigte Dritte.
- Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit der Daten und Prüfbarkeit der Verfahren.



Jede verantwortliche Stelle hat die bei ihr gespeicherten Daten vor Verlust, Verfälschung oder unberechtigtem Zugriff gesichert aufzubewahren. Das erfordert von den Mitarbeitern eine erhöhte Aufmerksamkeit beim Transport von Daten, beim Umgang mit dem Passwort, dem Verschluss der Unterlagen gegen unberechtigte Einsicht und bei der Kontrolle von Dienstleistern (Reinigungsunternehmen, Datenentsorgung, DV-Wartung).

Die durch die DV-Abteilung in Zusammenarbeit mit den Fachabteilungen vorgesehenen Zugriffsschutz- und Datensicherungsfunktionen sind auch aus datenschutzrechtlicher Sicht mit Sorgfalt umzusetzen. Insbesondere sind die Zugriffsrechte restriktiv (eingeschränkt) zu handhaben, die Passworte vertraulich zu behandeln und die vorgeschriebenen Datensicherungsmaßnahmen der jeweiligen Anwendung angemessen einzuhalten.

Dabei sind die bekannten betrieblichen Regelungen durch die jeweils damit Beschäftigten strikt zu beachten.

Aufgaben des betrieblichen Datenschutzbeauftragten

- Hinwirken auf die Einhaltung des Datenschutzes im Unternehmen

Der betriebliche Datenschutzbeauftragte wird in vertrauensvollem Zusammenwirken mit allen Mitarbeiterebenen datenschutzrechtliche Probleme erkennen und den Verantwortlichen Empfehlungen zur betrieblichen Umsetzung geben.

Er ist bei der Durchführung der Maßnahmen von den Fachbereichen zu unterstützen und über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu informieren. Bei der Verarbeitung sensibler Daten oder bei der DV-gestützten Erstellung von Persönlichkeitsprofilen hat er eine Vorabkontrolle durchzuführen.

Die notwendigen Angaben für das Verfahrensverzeichnis sind dem Datenschutzbeauftragten mitzuteilen. Der Datenschutzbeauftragte hat es zur Einsicht für jedermann bereitzuhalten, wobei das Unternehmen zum Schutz von Betriebs- und Geschäftsgeheimnissen eine auf die zwingend erforderlichen Angaben komprimierte Version des Verfahrensverzeichnisses zur "Auskunft an Jedermann" bereithält.

Der betriebliche Datenschutzbeauftragte unterliegt einer besonderen Verschwiegenheitspflicht und hat ein Zeugnisverweigerungsrecht, von dem er nur vom Betroffenen entbunden werden kann. Er steht allen Mitarbeitern für ihre Fragen und Anregungen zur Verfügung und ist insbesondere auf ihre Akzeptanz und Unterstützung angewiesen.

Mit freundlichen Grüßen
i.A.
Wolfram Fähnrich
Betrieblicher Datenschutzbeauftragter wolfram.faehnrich@lsb-nrw.de