Hans G. Zeger[1],

Vereinsbestimmungen Datenschutz

Neben den allgemeinen Datenschutzbestimmungen, die für Vereine genauso, wie für kommerzielle oder behördliche Datenverarbeiter gelten, ergeben sich oft einige Spezialfragen, die aus Vereinskooperationen oder dem Fund-Raising entspringen - Für den Datenschutz ist es jedoch unerheblich, ob Daten aus kommerziellen oder nichtkommerziellen (gemeinnützigen) Zwecken ermittelt, verwendet oder übermittelt werden.

Die wichtigsten allgemeinen Bestimmungen:
- Registrierungspflicht (sofern nicht eine Standardanwendung genügt)
- Besondere Verpflichtungen bei der Einschaltung eines Dienstleisters,
- Haftung des Auftraggebers
- Auskunftspflicht gegenüber dem Betroffenen
- Richtigstellungs- und Löschungsrechte

Weiters ergeben sich bei Vereinen eine Reihe von Spezialfragen:
- Dürfen gleichartige Vereinigungen über einem Dachverband Interessentendaten austauschen?
- Dürfen Mitgliederdaten 'vereinsintern' weitergegeben werden?
- Was geschieht mit Daten nach Vereinsauflösung?
- Wie ist Missbrauch eigener (Adress)daten zu verhindern?
- Was sind öffentlich zugängliche Informationen?

Darüber hinaus kann die Verwendung von personenbezogenen Daten zu wissenschaftlichen oder statistischen Zwecken von Bedeutung sein.

Eine abschliessende Behandlung aller Datenschutzfragen ist gerade bei Vereinen nicht möglich. Unterschiedliche Vereinszwecke, Mitgliederstrukturen und Finanzierungsmodelle führen zu unterschiedlichsten datenschutzrechtlichen Konstellationen. Details zu allen Datenschutzthemen finden sich auf der Website der ARGE DATEN (www.argedaten.at), Beratung erhalten Mitglieder der ARGE DATEN.

mehr --> http://seminar.argedaten.at
mehr --> http://privacy.argedaten.at

Dürfen personenbezogene Daten ohne Registrierung verwendet werden?

(DSG 2000 § 4, § 7, § 17, § 52)
Grundsätzlich ist die Registrierung beim Datenverarbeitungsregister (DVR)Voraussetzung für die Verwendung personenbezogener Daten in Unternehmen (vgl. §17 DSG 2000). Die Verwendung von Daten umfasst dabei das Ermitteln, das Verarbeiten und die Übermittlung von personenbezogenen Daten (vgl. §4 DSG 2000).

Um zu verhindern, dass jede Organisation / jedes Unternehmen für alltägliche Aufgaben jeweils Registrierungen vornehmen muss, wurden sogenannte Standardanwendungen definiert, die von der Registrierungspflicht ausgenommen sind. Im Unternehmensbereich sind dies insbesondere die Verwaltung von Personaldaten, Kunden- und Lieferantendaten. Im Vereinsbereich ist es die Mitgliederverwaltung. Solange diese Daten im Rahmen der Standardanwendungen verwendet werden, ist keine Registrierung notwendig.

---

1 Der Autor ist Geschäftsführer der "e-commerce monitoring GmbH", Lektor an der TU-Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Obmann der "ARGE DATEN"

Die Standardanwendungen geben auch vor, an wen solche Daten übermittelt werden dürfen. In in diesen vorgegebenen Fällen ist auch die Übermittlung von Daten ohne Registrierung zulässig.

Eine praktisch sehr bedeutsame Ausnahme von der Registrierungspflicht sind die Adressdaten von Kunden. Diese dürfen von Unternehmen an Adressverlage und Direktwerbeunternehmen übermittelt werden, ohne dass eine Registrierung notwendig wäre.

Die Verwendung von Datenarten, die nicht von einer Standardanwendung erfasst sind, bzw. die Übermittlung an Empfänger, die in einer Standardanwendung nicht vorgesehen sind, bedarf in jedem Fall einer Registrierung. Für bestimmte Daten, insbesondere sensible Daten, ist sogar eine Vorabkontrolle durch die Datenschutzkommission vorgesehen. Jede Ermittlung, Verarbeitung oder Übermittlung solcher Daten ohne Registrierung ist unzulässig. Ebenso unzulässig wäre natürlich eine Verwendung von Daten, die über den in der Registrierung festgelegten Rahmen hinausgeht. Für die unzulässige Verwendung von personenbezogenen Daten sind im DSG 2000 Verwaltungsstrafen bis zu EUR 18.890 vorgesehen.

Um die Zulässigkeit der Verwendung von Daten ohne Registrierung festzustellen, ist also eine genaue Analyse der jeweiligen Umstände notwendig.

Die Unterscheidung lässt sich auch an einem Beispiel zeigen: Wenn das Unternehmen A personenbezogene Daten von eigenen Kunden an ein Unternehmen B übermittelt, ist dies zulässig, weil in diesem Fall die oben genannte Ausnahme greift. Die Übermittlung z.B. von Interessentendaten wäre hingegen nicht zulässig, weil zwar Unternehmen selbst Daten von Interessenten verarbeiten dürfen, eine Übermittlung ohne Registrierung allerdings in der Standardanwendung nicht vorgesehen ist. Außerdem wäre in einem solchen Fall auch die Verwendung durch das Unternehmen B als Übermittlungsempfänger nicht zulässig (vgl. §7 DSG 2000).

Für Betroffene ist die Zulässigkeit der Verwendung von personenbezogenen Daten ohne Registrierung bei der Durchsetzung ihrer Betroffenenrechte ein Nachteil. Durch die fehlende Registrierung wird ein Überblick über die bei verschiedenen Auftraggebern verarbeiteten Daten und eventuelle Übermittlungen erschwert.

Das Datenverarbeitungsregister ist Teil der Datenschutzkommission.

mehr --> http://www.argedaten.at/office/recht/dsg2000.htm

Unter welchen Umständen ist eine Zustimmung eines Betroffenen gültig?

(DSG 2000 § 4, DSG 2000 § 8, DSG 2000 § 9)
In vielen Fällen benötigt man für die Verwendung der Daten die Zustimmung des Betroffenen. Dies wird dann der Fall sein, wenn die Datenverwendung weder gesetzlich vorgeschrieben ist, noch sich aus einem Vertragsverhältnis ergibt. Viele Datenübermittlungen sind nur mit Zustimmung des Betroffenen erlaubt.

Das DSG sieht für die Gültigkeit der Zustimmung vor, dass dieser in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligen muss.

Dies bedeutet konkret, dass ein Betroffener einer Datenverwendung nur dann gültig zustimmen kann, wenn er weiß, welche Daten zu welchem Zweck verwendet werden. Die Zustimmung bezieht sich folglich nur auf diesen Zweck, so dass z.B. bei der Verwendung von Daten bei demselben Auftraggeber für einen anderen Zweck eine neuerliche Zustimmung des Betroffenen notwendig wäre.

Eine schriftliche Zustimmung des Betroffenen ist gesetzlich nicht zwingend vorgeschrieben, für einen leichteren Nachweis allerdings sehr empfehlenswert.

Eine weit verbreitete falsche Vorstellung ist, dass die freiwillige Zustimmung eines Betroffenen den berechtigter Zweck oder die Rechtsgrundlage für eine Datenanwendung ersetzen kann. Fehlt ein berechtigter Zweck oder ist die Verwendung der Daten rechtswidrig, so dürfen auch Daten, die vom

Betroffenen freiwillig zur Verfügung gestellt wurden oder zu der Verwendung der Betroffene seine Einwilligung gegeben hat, nicht verwendet werden. Dies mag zwar auf den ersten Blick die Privatautonomie des Einzelnen einschränken, ist aber notwendig, um die Ausübung direkten oder indirekten Zwangs zu verhindern.

Auch vom OGH wurden einige Fälle zur Gültigkeit von Zustimmungserklärungen entschieden (vgl. OGH 4Ob28/01y oder 6 Ob16/01y - 'Eine wirksame Zustimmung zur Verwendung nichtsensibler Daten liegt nur vor, wenn der Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden.').

Was ist ein Dienstleister im Sinne des DSG 2000?

(DSG 2000 §4 Z5, §10, §11)
Nach der Definition des DSG 2000 sind Dienstleister alle Personen, die Daten verwenden, die ihnen vom Auftraggeber einer Datenanwendung zur Erfüllung einer konkreten Aufgabe überlassen werden. In erster Linie fallen darunter Organisationen oder Personen, denen im Rahmen eines größeren Projekts, einer Tätigkeit, einzelne Datenverarbeitungsschritte übertragen wurden.

Es ist allerdings zu beachten, dass u.U. auch andere Personen oder Organisationen unter den Dienstleisterbegriff fallen. So ist z.B. bei der Durchführung von Reparaturen an EDV-Anlagen davon auszugehen, dass ein Zugriff auf Daten möglich ist und eine Dienstleistung vorliegt.

Für die Inanspruchnahme von Dienstleistern sind im DSG besondere Regelungen vorgesehen. So ist der Auftraggeber für die rechtmäßige und sichere Datenverwendung beim Dienstleister verantwortlich. Bei genehmigungspflichtigen Datenanwendungen ist auch die Beauftragung eines Dienstleisters genehmigungspflichtig.

Auch den Dienstleister treffene eine Reihe von Verpflichtungen, vor allem im Bereich der Datensicherheit. Außerdem ist es dem Dienstleister natürlich nicht erlaubt, die überlassenen Daten für andere als die vom Auftraggeber vorgesehenen - also insbesondere nicht für eigene - Zwecke zu nützen. Möchte ein Dienstleister selbst weitere Dienstleister heranziehen, hat er dies dem Auftraggeber mitzuteilen.

Das DSG sieht zudem vor, dass Vereinbarungen zwischen Auftraggeber und Dienstleister, die die obengenannten Pflichten betreffen, schriftlich festzuhalten sind (Dienstleistervereinbarung).

mehr --> http://www.argedaten.at/dsg2000

Haftung des Auftraggebers

Auf Grund des konkreten Anlassfalles soll die Verantwortlichkeit des Auftraggebers aufgezeigt werden. Im Rahmen eines Mountainbike-Rennens des Polizeisportvereins (siehe Stellungnahme unten) wurden die Daten der teilnehmenden Kinder (Name, Adresse und Geburtsdatum) auf einer Webseite veröffentlicht.

Der Polizeisportverein rechtfertigte sich damit, dass er dem Webseitengestalter nur den Auftrag gegeben hat, die Namen der Kinder, aber keine zusätzliche Information zu veröffentlichen.

Der Webseiten-Gestalter ist in diesem Sinn als Dienstleister gem. DSG 2000 §4 Z5 anzusehen. Im übrigen auch der Betreiber des Webservers selbst oder auch der InternetServiceProvider, der die Anbindung zum Internet herstellt und in letzter Konsequenz auch jeder InternetServiceBetreiber, der einem konkreten Benutzer den Zugang zu diesen Daten verschafft.

Der Polizeisportverein ist Auftraggeber gem. DSG 2000 §4 Z4, da er die Möglichkeit hat, im Rahmen der gesetzlichen Bestimmungen zu entscheiden, was mit den Teilnehmerdaten zu geschehen hat. Er könnte etwa entscheiden, dass die Namen nur im Rahmen der Durchführung des Rennens oder im Rahmen der örtlichen Siegerehrung verwendet werden oder dass nur die Vornamen veröffentlicht werden usw.

Die Kinder/Jugendlichen sind in diesem Zusammenhang als Betroffene anzusehen und es wird vom Alter und der Reife der Kinder/Jugendlichen abhängig, inwieweit sie ihre Betroffenenrechte selbst wahrnehmen können oder dies die Erziehungsberechtigten übernehmen müssen. Unter anderem könnte eine Beschwerde wegen Verletzung des Datengeheimnisses erhoben werden (DSG 2000 §1). Die Erziehungsberechtigten haben, wenn wir an kleinere Kinder denken, nicht die Möglichkeit nach eigenen Überlegungen Beschwerde einzuheben oder nicht, sondern nur in Hinblick auf mögliche Nachteile/Vorteile der Kinder. Mit anderen Worten, wenn eine Datenschutzverletzung vorliegt und diese das Kindeswohl gefährden kann, dann muß der Erziehungsberechtigte Beschwerde erheben!

Der Auftraggeber kann nun für die Besorgung einzelner Tätigkeiten Erfüllungsgehilfen, im Datenschutzgesetz etwas unklar, Dienstleister genannt, heranziehen. Er muß jedoch den Erfüllungsgehilfen geeignete Aufträge erteilen und Vorsorge treffen, dass diese Aufträge erfüllt werden und keine Verletzung des Datenschutzes und der Privatsphäre stattfindet. Dies wird etwa durch entsprechende Kontrollen erfolgen.

Im vorliegenden Fall rechtfertigt sich der Auftraggeber, der Polizeisportverein, damit, dass sich der Webgestalter nicht an seinen Auftrag gehalten hat und eigenmächtig die zusätzlichen Daten der Kinder veröffentlicht hat. Selbst bei weisungswidrigen Verhalten eines Dienstleisters bleibt jedoch die Haftung des Auftraggebers bestehen! Dies wird in Verwaltungsstrafverfahren, etwa vor der Datenschutzkommission oder bei Zivilverfahren, vor Gericht, von Bedeutung sein.

Der Auftraggeber kann allenfalls, wenn ein materieller Schaden gegeben ist, diesen Schaden vom Dienstleister im Regreßweg zurückfordern. Auch eine strafrechtliche Verantwortlichkeit des Dienstleisters könnte gegeben sein. Dazu müßte aber Vorsatz nachgewiesen werden und die Veröffentlichung geeignet sein, einen Schaden zu erzielen oder der Täter hätte sich einen Vermögensvorteil verschafft (DSG 2000 §51). Ein derartiger Vermögensvorteil wäre schon dann gegeben, wenn ein Dienstleister ihm überlassene Daten an einen Adressenverlag verkauft oder durch die 'Mehrarbeit' die aus der Veröffentlichung zusätzlicher Daten entstehen, ein Mehrentgelt bezieht.

Im konkreten Fall wäre der Polizeisportverein gut beraten zu prüfen, ob die Daten vom locker agierenden Webgestalter nicht zu einem Vermögensvorteil führten.

mehr --> http://www.argedaten.at/office/recht/dsg204__.htm
mehr --> http://www.argedaten.at/office/recht/dsg210__.htm

Was bedeutet des 'Recht auf Auskunft'?

(DSG 2000 §26)
Jeder Betroffene hat bei jedem Auftraggeber das Recht einmal im Jahr kostenlos Auskunft über alle aktuellen Daten zu erhalten, die der Auftraggeber über ihn verwendet. Diese Auskunft hat in allgemein verständlicher Form zu erfolgen, d.h. ohne unverständliche Codes und Abkürzungen.

Die Frist für die Auskunft beträgt 8 Wochen. Innerhalb dieser Zeit muss entweder eine vollständige Auskunft gegeben werden oder der Auftraggeber muss begründen, warum er keine Auskunft gibt.

Es genügt auch nicht nur die Datenarten, wie 'Name', 'Adresse', 'Bonitätsdaten' bekannt zu geben, sondern es müssen die genauen Daten, z.B.: Name = Hermann Müller, Bonität = 100 (von 0-100, wobei 100 beste Bonität bedeutet), angegeben werden.

Um erfolgreich Auskunft zu erhalten, sind für den Betroffenen zwei wesentliche Punkte zu beachten.

Erstens muss er seine Identität nachweisen. In der Regel genügt bei öffentlich-rechtlichen Auftraggebern dazu die Bekanntgabe von Name, Adresse und Geburtsdatum. Die Auskunft wird dann mittels Rsa- oder Rsb-Brief zugestellt, die Identitätsprüfung übernimmt der Briefträger. Bei privat-rechtlichen Auftraggebern, zu denen vertragliche Vereinbarungen existieren (z.B. Banken, Versicherungen, Hausverwalter, Arbeitgeber, ...) wird der Hinweis auf die Unterschrift und der Möglichkeit eines Unterschriftsvergleiches genügen. Auch die

persönliche Abholung einer Auskunft gegen Vorlage eines amtlichen Dokuments ist möglich. Bei einzelnen Auftraggebern kann es auch notwendig sein, andere Formen des Identitätsnachweises zu beachten.

Zweitens muss der Betroffene bei der Auskunftserteilung mitwirken. Dies kann dadurch geschehen, dass der Betroffene umschreibt in welcher Beziehung er zum Auftraggeber steht (etwa als Kunde, Mitarbeiter, Lieferant, Empfänger eines Briefes, ...) oder indem er angibt, in welchen Datenverarbeitungen laut Registrierung beim DVR er als Betroffener enthalten sein könnte.

Um die Auskunftsverfahren möglichst zu beschleunigen, empfiehlt es sich, eine gemischte Strategie anzuwenden. Der Betroffene soll einerseits in allgemeinen Formulierungen angeben, in welcher Beziehung er zum Auftraggeber steht, weiters sollten die gewünschten Datenanwendungen möglichst genau beschrieben werden und zusätzlich sollten - falls verfügbar - die registrierten Datenanwendungen in denen man enthalten sein könnte, genannt werden.

Empfohlen wird, sowohl das Auskunftsbegehren zu Beweiszwecken schriftlich zu stellen (eingeschrieben) als auch die Auskunft schriftlich zu verlangen.

Sollte die Auskunft nicht erfolgen, nicht vollständig erfolgen, unverständlich sein oder unvollständig sein, dann kann dagegen eine Beschwerde bei der Datenschutzkommission eingebracht werden.

Die ARGE DATEN hat zum Auskunftsrecht einen Musterbrief verfasst, der entsprechend zu adaptieren ist.

Auf Grund der spezifischen Besonderheiten der Finanzdienstleister hat die ARGE DATEN auch einen speziellen Brief für Auskunftsanforderungen bei Banken und den Gemeinschaftseinrichtungen der Banken verfasst.

Weiters wurde ein eigener Brief zur Auskunftsanforderung für das Bundesministerium für Inneres und die Bundespolizeidirektionen verfasst.

Wann besteht ein Recht auf Berichtigung und Löschung von Daten?

(DSG 2000 §27)
Grundsätzlich sind nicht mehr aktuelle oder unrichtige Daten zu berichtigen und nicht mehr benötigte Daten oder unberechtigt ermittelte bzw. verwendete Daten zu löschen. Den Beweis zu erbringen, ob Daten richtig oder falsch ist, obliegt in der Regel dem Auftraggeber. Nur dann wenn der Auftraggeber nachweisen kann, dass die verwendeten Daten ausschließlich vom Betroffenen stammen, müssen Aktualisierungs- und Berichtigungswünsche des Betroffenen durch ihm belegt bzw. plausibel gemacht werden.

Wann ist zu aktualisieren?
Die Aktualisierung ist immer dann durchzuführen, wenn ein Datenverarbeiter Kenntnis von einer, für seine Zwecke wesentlichen, Änderung der Daten hat. Dies kann durch den Betroffenen erfolgen, aber auch indem Post retourniert wird oder Dritte auf veraltete oder falsche Daten hinweisen.

Muss ein Datenverarbeiter aktiv Daten nach veralteten oder falschen Daten suchen?
Dies hängt wesentlich vom Zweck der Datenverwendung ab. In einer bloß intern verwendeten Marketing- und Interessentendatei wird es nicht notwendig sein, ständig Anschrift, Telefonnummer, Fax, ... nach der Aktualität zu überprüfen. Bei der nächsten Verwendung oder Postaussendung wird man auf Grund der Retouren und missglückter Kontakte feststellen, welche Daten nicht mehr aktuell sind und diese korrigieren.

Wesentlich verschärft sind die Aktualisierungspflichten, wenn Daten auch für Dritte bereitgestellt werden oder sogar veröffentlicht werden.

Hier wird sowohl eine regelmäßige Überprüfung von zeitbezogenenen Daten stattfinden müssen. Ebenso wird die gesamte Datenverarbeitung so zu konzipieren sein, dass das Veralten von Daten erkannt und vermieden werden kann. Wenn jemand Daten von einem Dritten zu einem bestimmten Zeitpunkt übernimmt und keine Maßnahmen setzt, wie diese Daten regelmäßig aktualisiert werden können, handelt er bei der Erfüllung der Aktualisierungspflicht sicher fahrlässig, möglicherweise auch grob fahrlässig.

Im üblichen geschäftlichen Umfeld, bei Kunden-, Lieferanten- oder Interessentenbeziehungen macht das Aktualisierungsrecht kaum Probleme.

Schwierigkeiten entstehen dort,
(a) wo Dritte, aus eigenem Antrieb Daten für eigene Zwecke sammeln oder
(b) wo Daten an Dritte für Zwecke weitergegeben werden (nicht immer im Interesse des Betroffenen).

Ein typisches Beispiel zu Fall (a) sind die Unmengen von Verzeichnissen, Datenbanken und Linklisten, die im Internet als Telefonbücher, Mail-Verzeichnisse oder Branchenverzeichnisse existieren. Meist werden diese Daten einmal übernommen und nicht mehr weiter gepflegt. Alte Informationen können Benutzer in die Irre führen oder sind schlicht ärgerlich.

Manche dieser Online-Verzeichnisse halten Update-Funktionen bereit, mit denen Betroffene selbst Daten pflegen können, die meisten ermöglichen keinerlei Online-Änderungen. In der Regel wird das bloße Bereitstellen einer Updatefunktion nicht ausreichen, sondern der Anbieter muss eigene Maßnahmen zur Erfüllung der Aktualisierungspflicht treffen. Dies umso mehr, als viele Betroffene gar nicht wissen, dass sie in einem bestimmten Informationssystem enthalten sind.

Wesentlich schwerwiegender ist Fall (b), etwa im Zusammenhang mit Wirtschaftsauskunftsdiensten und Gläubigerschutzverbänden. Falsche oder veraltete Daten können kreditschädigend sein oder den Zugang von Personen zum wirtschaftlichen Leben verteuern oder unmöglich machen. Vielfach melden Finanzdienstleister an den KSV 1870, dass sie 'Kreditanträge abgelehnt' hätten oder ein Kunde in 'Zahlungsverzug geraten sei', ohne die tatsächlichen Begleitumstände darzulegen bzw. festzuhalten, wie aktuell diese Information ist. Hier besteht von Seiten des Betroffenen eine Aktualisierungs- und Klarstellungsrecht, dass alle notwendigen Begleitumstände derartiger schwerwiegender Feststellungen darlegt. Aber auch von Seiten des meldenden Geldinstituts und auch des KSV besteht eine aktive Aktualisierungspflicht. In regelmäßigen Abständen, empfohlen wird mindestens halbjährlich, haben diese Stellen zu überprüfen, ob die gespeicherte, verwendete und veröffentlichte Information noch vollständig richtig ist. Kredite können ganz oder teilweise zurückgezahlt sein, ein Zahlungsverzug kann bereinigt sein, bei Zahlungsproblemen kann es zu einer einvernehmlichen Lösung zwischen Betroffenen und Bank gekommen sein.

Nach den bisherigen Erfahrungen stehen Auftraggeber im Bereich der Wirtschaftsauskunftsdiensten meist auf dem Standpunkt, dass alles was sie tun 'berechtigt' ist, und agieren bei der Korrektur und Löschung von veralteten Informationen jenseits der gesetzlichen Regelungen. Generelle Verhaltensregeln und Empfehlungen bei der Ablehnung eines Löschungs- und Aktualisierungswunsches können keine gegeben werden, ob ein Aktualisierung- bzw. ein Löschungswunsch Erfolgsaussichten hat, muss im Einzelfall analysiert werden. Die ARGE DATEN ist aber gerne bereit, bei entsprechend gut dokumentierten Fällen zu intervenieren.

Berichtigungen und Löschungen haben binnen 8 Wochen zu erfolgen. Sollten Sie nicht durchgeführt werden, ist innerhalb dieser Frist zu begründen, warum nicht.

Was darf/muss ein Datenverarbeiter zur Aktualisierung von personenbezogenen Daten tun?

(DSG 2000 §27)
Eine aktive Aktualisierungspflicht, also das selbständige Nachforschen, ob Informationen noch richtig sind, wird einem Datenverarbeiter - abhängig vom Zweck - im wirtschaftlich zumutbaren Ausmaß zukommen.

Grundsätzlich ist kein Datenverarbeiter verpflichtet, täglich alle Informationen aktiv nach ihrer Gültigkeit zu überprüfen. Jeder Datenverarbeiter ist aber verpflichtet ein technisches und organisatorisches System zu entwickeln, daß die Aktualisierungen im notwendigen Ausmaß sicherstellt.

Viele seriöse Datenverarbeiter stehen vor dem Problem die Aktualisierungspflichten nach DSG 2000 §27 angemessen zu erfüllen. Es sind viele Unternehmen von sich aus interessiert (Vermeidung von Portokosten, Streuverluste in der Werbung, ...) 'Karteileichen' und doppelte Datensätze zu erkennen und zu entfernen.

Welche Hilfsmittel dürfen sie dazu verwenden?
Sicher zulässig sind Auswerte- und Abgleichprogramme, die etwa phonetische Unterschiede erkennen und entfernen. Sicher zulässig ist es auch, verschiedene eigene, bisher getrennte Datenbestände eines Geschäftsbereiches miteinander zu verknüpfen und abzugleichen. Auch eigene Recherchen, wie Telefonanrufe bei eingetragenen Kunden und Interessenten, schriftliche Anfragen, Online-Recherchen, die Auswertung von veröffentlichten Telefonanschlußdaten (=Telefonücher) oder auch der Zukauf von Adressen, etwa von der Wirtschaftskammer (Geschäftsdaten) oder von einem Adressenverlag werden erlaubt sein.

Problematisch wird es bei der Benutzung öffentlich-rechtlicher Datenbestände, also Informationen, die für gänzlich andere Zwecke vorgesehen sind, etwa die Meldeevidenz, die Wählerevidenz oder die Grundstücksdatenbank. Im Zuge gezielter Abfragen nach bestimmten Personen wird es auch hier zulässig sein, diese Daten zur Aktualisierung eigener Informationen zu verwenden, eine generelle Übernahme dieser Daten und eines Abgleichs mit den eigenen Informationen wird jedoch im Regelfall nicht erlaubt sein.

Das Beispiel der Meldeevidenz macht dies deutlich. Die Meldepflicht hat den Zweck, von jedem Bürger eine ladungsfähige Adresse zu haben. Diese Adresse ist nach dem Meldegsetz ident mit seinem gewöhnlichen Aufenthalt. Als Kunde eines Versandhauses oder einer sonstigen Firma werde ich aber auch Waren an Adressen bestellen können bzw. dorthin liefern lassen können, wo ich nicht gemeldet bin. Für den Lieferant ist das Melderecht solange belanglos, als die Ware zuverlässig zugestellt werden kann und die Rechnungen bezahlt werden. Ein Abgleich mit den Meldedaten würde hier zusätzliche Fehler bringen. Erst wenn bei Zustellung oder Bezahlung etwas schief läuft, wird es vielleicht notwendig sein, auf Meldedaten zurückzugreifen. Um das zu können, muß sich der Lieferant jedoch schon vorher über die Identität und die Zahlungsfähigkeit einer Person vergewissert haben.

Im Ergebnis ist die Datenpflege ein mühevolles und personal- und zeitintensives Geschäft, das den eigentlichen Kostenfaktor bei der Verwaltung personenbezogener Daten darstellt.

Dürfen gleichartige Vereinigungen über einem Dachverband Interessentendaten austauschen?

Besonders bei Interessensvereinigungen tritt folgende Situation häufig auf. In einem Fachbereich, wie Sozialhilfe, Ernährung, Bildung, Kultur, Verkehr usw. bestehen mehrere, an sich unabhängige Vereinigungen. Diese entschließen sich nach einiger Zeit, zum Zwecke der verbesserten Koordination und Öffentlichkeitsarbeit, einen gemeinsamen Dachverband zu betreiben.

Der Dachverband organisiert vorerst bloß gemeinsame Presseerklärungen, Veranstaltungen, Workshops usw., gibt aber nach einiger Zeit auch eine eigene Zeitschrift heraus, hat eigene Mitglieder und möchte auch die Mitglieder der Gründungsvereinigungen direkt informieren. Dazu werden deren Mitgliederadressen benötigt.

Datenschutzrechtlich handelt es sich bei jedem Gründerverein und beim Dachverband um voneinander unabhängige Organisationen. Personenbezogene Daten haben diese Organisationen für ganz bestimmte eigene Zwecke, wie Mitgliederbetreuung, Abonenntendienst, Warenversand, ... ermittelt.

Wenn nichts anderes vereinbart wurde, und dies ist in der Regel bei langjährig existierenden Vereinen der Fall, dürfen die Daten nur innerhalb dieses Vereins zu den ausdrücklich überlassenen Zwecken verwendet werden. Eine Weitergabe an einen Dachverband, ist genauso wie die Weitergabe an 'Schwester'vereinigungen oder völlig fremde Organisationen, nur durch Zustimmung des Betroffenen möglich. Auch gleichartige Statuten oder gleiche 'Themen' erleichtern nicht die Datenweitergabe.

Wie könnte nun die Aussendung einer Dachverbandszeitung an die Mitglieder der Gründungsvereine organisiert werden?

Eine Möglichkeit ist, daß der Dachverband schlicht die entsprechende Zahl von Zeitschriften an den jeweiligen Gründerverein übergibt und dieser bei der nächsten eigenen Aussendung die Zeitschrift beilegt. Eine zweite - zulässige - Möglichkeit ist, daß die Adreßdaten des Gründervereines dem Dachverband ausschließlich zum Zweck des verschickens der Dachverbandszeitschrift ÜBERLASSEN werden. Der Dachverband darf diese Daten zu keinem anderen Zweck aufbewahren, abgleichen oder sonstwie verwenden.

Nachteil beider Möglichkeiten ist, daß Personen, die bei drei gleichartigen Vereinigungen Mitglied sind, unter Umständen die Dachverbandszeitung dreimal unabhängig voneinander zugeschickt erhalten. Dies ist unwirtschaftlich und kann auch von den Betroffenen als lästig empfunden werden.

Wir raten daher zu folgender klaren und unbedenklichen Vorgangsweise:

- Für neue Mitglieder sollte schon im Mitgliedsantrag eine Zustimmungsmöglichkeit vorgesehen werden, daß sie auch Informationen eines bestimmten Dachverbandes erhalten.

- Bestehende Mitglieder sollten im Rahmen regelmäßiger Aussendungen auf dieses neue Informationsangebot aufmerksam gemacht werden und die Möglichkeit haben, ihre Zustimmung zur Datenweitergabe an den Dachverband zu geben.

- Beim - wie oben bechriebenen - Erstversand der angesprochenen Dachverbandszeitung sollte eine Feedback-Möglichkeit vorgesehen werden, daß sich der Betroffene direkt beim Dachverband zum Bezug der Zeitung anmelden kann.

Die Daten aller Personen, die weder einer Datenweitergabe zustimmen, noch sich direkt an den Dachverband wenden, wird man nicht für derartige gemeinsame Aktivitäten verwenden dürfen.

Grundsätzlich könnte auch die Generalversammlung eines Vereines beschließen, daß die Datenweitergabe an einem Dachverband oder an befreundete 'Schwester'organisationen als wesentlicher Teil des Vereinszweckes anzusehen sind und daher nicht individuell zustimmungsfähig ist. Ohne alle Details zu berücksichtigen, wird in diesem Fall für Mitglieder, die vor einer derartigen Statutenänderung beigetreten sind, ein sofortiges Austrittsrecht bestehen.

Dürfen Mitgliederdaten 'vereinsintern' weitergegeben werden?

Ob Mitgliederdaten zwischen Vereinsmitgliedern ausgetauscht werden dürfen, hängt im Wesentlichen von drei Faktoren ab:

1. vom Vereinszweck / von den Vereinsstatuten
2. von der Vereinsgröße
3. von den Mitgliedervereinbarungen

ad 1. Ist in den Vereinsstatuen ausdrücklich festgehalten, daß einer der Vereinszwecke das Knüpfen von Kontakten der Mitglieder untereinander ist - aus welchen Gründen auch immer - dann wird einem Datenaustausch im Ausmaß des Vereinszweckes nichts entgegenstehen.

ad 2. Ist ein Verein, etwa ein lokaler Tennis- oder Kegelklub so klein, daß 'jeder jeden kennt', dann wird auch einem Datenaustausch in dem Ausmaß als sich die Leute sowieso untereinander kennen (bzw. kennen sollten) nichts im Wege stehen.

ad 3. Treffen weder der erste, noch der zweite Fall zu, dann wird eine Weitergabe von Mitgliederdaten nur dann zulässig sein, wenn die einzelnen Mitglieder dieser Weitergabe zustimmen. Da die Adressenweitergabe bzw. der Datenaustausch offensichtlich kein zentrales Vereinsanliegen ist (sonst würde ja 1. gelten), könnte bei einer Verweigerung der Zustimmung auch keine Sanktion gesetzt werden.

Im übrigen ist es unerheblich in welcher technischen Form die Datenweitergabe erfolgt. Ist die Weitergabe als gedrucktes Verzeichnis zulässig, dann ist sie es auch in elektronischer Form. Oder umgekehrt, ist die elektronische Weitergabe unzulässig, dann dürfen die Daten auch nicht ausgedruckt weitergegeben werden.

Wie ist der Missbrauch von Daten zu verhindern?

Vielfach werden Daten 'außer Haus' verarbeitet, sei dies zu Zwecken der Buchhaltung oder Lohnverrechnung, aber auch um Mailings und Postzusendungen durchzuführen. Viele Datenverarbeiter machen sich Sorgen bezüglich des Missbrauchs ihrer Daten.

Grundsätzlich ist für jede Datenverwendung der Auftraggeber verantwortlich. Zieht er für bestimmte Aufgaben, die er nicht oder nicht kostengünstig genug selbst erledigen kann, Dienstleister heran, dann haftet er für deren korrektes Verhalten.

Es liegt in der Regel im eigenen Interesse der Datenverarbeiter, dass mit den wertvollen Daten kein Missbrauch betrieben wird.

Die Überlassung der Daten, etwa an einen Steuerberater, wird generell unproblematisch sein, da hier verschärfte Berufspflichten sicherstellen, dass Missbrauch so weit als möglich reduziert wird.

Anders ist es bei der Abwicklung der Mailings. Druckereien oder Versandunternehmen haben oft Zugang zu den wertvollen Adressdaten. Oft bieten Adressenverlage diese Dienstleistungen auch für fremde Datenbestände an.

Die, mittels Internet übertragenen oder per CD übergebenen Daten sind rasch kopiert und viele Firmen, aber auch gemeinnützige Vereine fragen sich, ob ihr Dienstleister der Versuchung einer raschen Kopie widersteht.

Eine Reihe von Sicherheitsmaßnahmen kann die Gefahr der missbräuchlichen Nutzung drastisch reduzieren:

(1) Auswahl eines geeigneten Dienstleisters
Man sollte über einen Anbieter Erkundigungen einziehen, ob schon Datenschutzbeschwerden vorlagen, eventuell könnte man auch eine Erklärung einfordern, dass das Unternehmen noch in keinem Datenschutzverfahren verwickelt war.

(2) Abschluß einer geeigneten Diesntleistervereinbarung
Die ARGE DATEN hat dazu ein Muster entwickelt, das als Basis genutzt werden kann.

(3) Verbot von Subunternehmern
Stellen sie sicher, dass das beauftragte Unternehmen selbst den Auftrag durchführt und nicht bloß weitervermittelt

(4) Laufende Kontrollrechte
Behalten sie sich vor, jederzeit, auch ohne Verdachtsmomente, die sichere Verwendung ihrer Daten kontrollieren zu dürfen

(5) Pönalevereinbarung
Vereinbaren sie eine relativ hohe Pönale, falls nachgewiesen wird, dass ihre Daten missbräuchlich verwendet wurden. Die Vereinbarung hat in der Regel nur abschreckende Wirkung, da der Beweis, dass tatsächlich der Dienstleister für einen Missbrauch verantwortlich ist, oft sehr schwer zu führen ist.

(6) Kontrolldaten

Benutzen sie die Adressen vertrauenswürdiger Personen um feststellen zu können, wann sie unerwünschte Zusendungen erhalten. Dieser Mechanismus funktioniert jedoch nur bedingt. Sehr viele Adressenverlage sind imstande leicht veränderte (sozusagen markierte) Namen und Anschriften zu erkennen und zu standardisieren. Kontrolladressen können dadurch herausgefiltert werden. Jedenfalls sollte eine größere Zahl von Adressen verwendet werden, etwa 100 Adressen, oder bei kleineren Mengen 1-3% der Gesamtzahl. Auch mit Kontrolldaten ist ein Missbrauch schwer zu beweisen, das Wissen um diese Daten hat jedoch meist eine abschreckende Wirkung.

mehr --> http://www.argedaten.at/muster/dsgdl01.html
mehr --> http://www.argedaten.at/news/pw20031009.html#4
mehr --> http://www.argedaten.at/office/recht/dsg211__.htm

Unter welchen Umständen ist die Verwendung von personenbezogenen Daten in wissenschaftlichen Studien zulässig?

(DSG 2000 § 7, § 46)
Bei der Durchführung von wissenschaftlichen Studien, Befragungen oder anderen Untersuchungen fallen sowohl in privaten als auch öffentlichen Institutionen sehr oft Daten an, die für Dritte unter Umständen sehr nützlich sein können. Ob eine solche Weitergabe zulässig ist, hängt von verschiedenen Faktoren ab.

Bei der Durchführung von wissenschaftlichen Studien, Befragungen oder anderen Untersuchungen fallen sowohl in privaten als auch öffentlichen Institutionen sehr oft Daten an, die für Dritte unter Umständen sehr nützlich sein können. Ein Beispiel für eine solche weitergehende Nutzung wären wissenschaftliche Forschungsprojekte, die sehr oft auf freiwillig zur Verfügung gestellte Daten angewiesen sind. Eine weitere Verarbeitung der Daten kann auch für den Auftraggeber positive Effekte bringen.

Es stellt sich daher die Frage, ob eine Weitergabe von Daten für solche Zwecke grundsätzlich gerechtfertigt ist. Die Antwort auf diese Frage hängt von verschiedenen Faktoren ab.

Zunächst ist zwischen personenbezogenen und nicht-personenbezogenen Daten zu unterscheiden. Bei Daten, die völlig anonymisiert sind und damit keinen Personenbezug mehr aufweisen, ist eine Weitergabe in der Regel problemlos möglich. Solche Daten fallen normalerweise nicht in den Geltungsbereich des Datenschutzgesetzes.

Bei direkt oder indirekt personenbezogenen Daten ist - unter der Voraussetzung, dass die Daten beim ursprünglichen Auftraggeber zulässigerweise verarbeitet werden - eine Weitergabe grundsätzlich nur möglich, wenn ein entsprechender Zweck für die Übermittlung besteht, die Übermittlung an einen berechtigten Empfänger erfolgt und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht gefährdet werden (§7 DSG 2000).

Speziell für wissenschaftliche und statistische Zwecke sind in den §46 und §47 DSG 2000 allerdings Ausnahmen vorgesehen.

Für Forschungsprojekte, die keine personenbezogenen Ergebnisse zum Ziel haben, dürfen öffentlich zugängliche, für andere Zwecke beim selben Auftraggeber rechtmäßig ermittelte und indirekt personenbezogene Daten verwendet und damit auch übermittelt werden.

Für andere Forschungsprojekte dürfen Daten, die nicht öffentlich zugänglich sind nur aufgrund gesetzlicher Vorschriften, mit Zustimmung der Betroffenen oder mit Genehmigung der Datenschutzkommission verwendet werden.

Eine Genehmigung der Datenschutzkommission setzt voraus, dass entweder die Einholung der Zustimmung der Betroffenen nicht oder nur mit unzumutbarem Aufwand möglich ist, ein öffentliches Interesse an den Ergebnissen der Forschung gegeben ist und der Antragsteller nachweist, dass er fachlich für die Durchführung des geplanten Forschungsprojektes geeignet ist.

Für die Verwendung sensibler Daten ist sogar ein wichtiges öffentliches Interesse nachzuweisen und es muss dafür gesorgt sein, dass die Personen, die mit sensiblen Daten zu tun haben, entweder einer gesetzlichen Verschwiegenheitspflicht unterliegen oder sonst ihre Verläßlichkeit glaubhaft machen können. Weiters kann die Datenschutzkommission in solchen Fällen eine Genehmigung nur mit zusätzlichen Auflagen oder unter besonderen Bedingungen erteilen.
Beispiele für genehmigte Forschungsprojekte sind insbesondere Forschungen zur NS-Vergangenheit. Bei solchen historischen Forschungen werden sehr oft personenbezogene – und teilweise auch sensible – Daten verwendet (Entscheidungen der DSK zu diesem Thema: K202.017/002-DSK/2002, K202.010/002-DSK/2001, 202.001/3- DSK/00).

Zusätzlich schreibt das Datenschutzgesetz allerdings vor, dass wenn in einzelnen Phasen eines Forschungsprojekts indirekt personenbezogene oder nicht-personenbezogene Daten für die Zwecke des Forschungsprojekts ausreichen, personenbezogene Daten zu verschlüsseln sind. Weiters muss der Personenbezug gänzlich beseitigt werden, sobald er nicht mehr notwendig ist.

mehr --> http://www.argedaten.at/office/recht/dsg2000.htm

Vereinsauflösung - Wohin mit den Daten?

(DSG 2000 §7, §24, §27)
Eine Weitergabe von Mitglieder- oder Mitarbeiterdaten wird nur mit Zustimmung der Betroffenen zulässig sein oder wenn die Nachfolgeorganisation den Vereinszweck in gleichartiger Weise weiterführt. Zur Gleichartigkeit wird unter anderem auch die Gemeinnützigkeit gehören. Bei einem Übergang von einem Verein zu einer kommerziell geführten gmbh wird diese Weiterführung nur in den seltensten Fällen gegeben sein.

Üblicherweise ist in den Statuten geregelt, wer bei Vereinsauflösung der Begünstigte für das Vereinsvermögen ist. Dies wird meist mit einer allgemeinen Formulierung, wie 'Dieses Vermögen soll, soweit dies möglich und erlaubt ist, einer Organisation zufallen, die gleiche oder ähnliche Ziele wie dieser Verein verfolgt.' geregelt. Meist entscheidet dann die Generalversammlung wer dieser Begünstigte ist. Oft wird ein Verein nicht schlicht aufgelöst, sondern geht in eine neue Rechtsform über oder fusioniert mit einer anderen Organisation, die Vermögensregelung ergibt sich dann aus dieser Übergangsvereinbarung.

In vielen Fällen verfügen Vereine auch über umfangreiches - personenbezogenes - Datenmaterial, meist Mitgliederdaten, Interessentendaten, eventuell auch Kundendaten, Daten über Mitarbeiter, Referenten, Lieferanten usw.

Diese Daten besitzen zwar oft einen hohen 'Wert', da sie viele Informationen über Interessenten enhalten, können aber nicht einfach dem Vermögen zugerechnet werden.

Es ist zu beachten, daß jede Organisation nicht einfach personenbezogene Daten besitzt. Alle personenbezogenen Daten, egal in welcher Form und mit welchem Aufwand sie erhoben wurden, dürfen immer nur in Hinblick auf einen bestimmten, rechtmäßigen Zweck verwendet werden. Datenverarbeiter 'besitzen' keine Daten, sondern sie verfolgen bestimmte Vereins- oder Unternehmenszwecke und im Zuge dieser Zwecke dürfen sie Daten verwenden. (DSG 2000 §7)

Fallen die Zwecke weg, die die ursprüngliche Verwendung der Daten rechtfertigten, dann dürfen die Daten nicht mehr verwendet werden und sind zu löschen (DSG 2000 §27).

Wird jedoch im Zuge der Vereinsauflösung mit einer Nachfolgeorganisation die Weiterführung bestimmter Bereiche und Tätigkeiten vereinbart und übernimmt diese Nachfolgeorganisation dazu die Verantwortung, dann dürfen die dazugehörigen Daten, die für den Betrieb dieser Tätigkeiten notwendig sind, ebenfalls an die Nachfolgeorganisation weitergegeben werden. Dies wird etwa bei einem Verein zutreffen, der umfangreiche Schulungs- und Ausbildungstätigkeit durchführte. Die diesbezügliche Interessentendatei wird einer Nachfolgeorganisation die dieselbe Art der Ausbildung anbietet, zu übergeben sein.

Die Details dieser Datenübergabe sind nicht genau geregelt, üblicherweise wird man aber die betroffenen Personen sowohl von der Vereinsauflösung, als auch von der Absicht, ihre Daten zur Weiterführung der bisherigen Tätigkeit an eine neue Organisation zu übergeben, informieren (DSG 2000 §24). Betroffene werden jedenfalls ein Widerspruchsrecht haben und sich gegen diese Datenweitergabe aussprechen können. Es ist daher dafür zu sorgen, daß die Betroffenen zeitgerecht informiert werden und genügend Zeit für einen Widerspruch haben.

Eine Weitergabe jener Daten, die sich auf die Mitgliedschaft des Vereins beziehen, wird nur möglich sein, wenn die Betroffenen dieser Weitergabe ausdrücklich zugestimmt haben. In der Regel bedeutet die Mitgliedschaft zu einem bestimmten Verein auch die Identifikation mit bestimmten Zielen und Ideen. Ob eine Nachfolgeorganisation dieselben Ziele verfolgt, kann nur jedes einzelne Vereinsmitglied selbst entscheiden.

Auch die Daten der Mitarbeiter eines Vereins werden nur mit deren Zustimmung weitergegeben werden dürfen. Die Entscheidung, bei einer neuen Organisation mitzuarbeiten oder sich von dieser Organisation anstellen zu lassen, ist eine persönliche Entscheidung, die jeder einzelne Mitarbeiter treffen muß.

Die Nachfolgeorganisation wird bezüglich der übermittelten Daten zum Auftraggeber und ist für die Einhaltung der Datenschutzregelungen verantwortlich. Dies bedeutet jedoch nicht, dass diese Daten nunmehr organisationsintern nach Belieben verwendet und mit anderen Daten verknüpft werden dürfen. Die Verwendung der Daten bleibt auf den ursprünglichen Zweck beschränkt.

Im übrigen gelten dieselben Regeln auch für Unternehmen die in Konkurs gehen oder fusionieren. Die vielfach kolportierten Unternehmensauflösungen und der 'Verkauf' des Datenbestandes aus der Konkursmasse kann in vielen Fällen schlicht eine Datenschutzverletzung darstellen.

