

# Datenschutz und Datensicherheit

Im Verein / in der Sektion

## Häufig gestellte Fragen

Prof. Dr. Rolf Lauser

Datenschutzbeauftragter (GDDcert)

Datenschutzauditor (GDD/BvD)

öbuv Sachverständiger für Systeme und Anwendungen der  
Informationsverarbeitung im kaufmännisch-administrativen Bereich  
sowie Datenschutz und Datensicherheit

# Schutzbereich des BDSG

- Grundlage des Datenschutzes:

Recht auf informationelle Selbstbestimmung.

Dieses leitet sich aus dem allgemeinen Persönlichkeitsrecht ab.

- Was ist geschützt?

Alle Daten über persönliche und sachliche Verhältnisse von natürlichen Personen (sog. personenbezogene Daten)

Daten juristischer Personen (Vereine, Verbände, Unternehmen) sind nicht geschützt.

Anonymisierte oder pseudonymisierte Daten (z.B. statistische Daten) sind ebenfalls nicht geschützt.

- Was sind personenbezogene Daten?

Adressen (Post, E-Mail- Telefonnummer)

Bankverbindungsdaten

Geburtsdatum

Beruf

Familienstand

## Schutzniveau des Datenschutzes

- Unterliegen alle personenbezogenen Daten dem gleichen Schutzniveau?

Nein. Es gibt personenbezogene Daten, die einem besonderen Schutz unterliegen und die nur mit einer ausdrücklichen Einwilligung des Betroffenen erhoben, verarbeitet, genutzt und an Dritte übermittelt werden dürfen.

Dazu gehören neben Gesundheitsdaten (dies ist ein Euphemismus und meint eigentlich Krankheitsdaten), auch Daten über die ethnische Herkunft, die politische Überzeugung und die sexuelle Orientierung.

Wenn solche Daten erhoben, also z.B. auf der Beitrittserklärung gesammelt werden sollen, dann ist es erforderlich, dass dem Betroffenen der Zweck der Datenerhebung bekannt gemacht wird und dieser eine dokumentierte Einwilligung zur Datenerhebung und Verarbeitung erteilt.

Sollen solche Daten an Dritte, d.h. an Fachverbände, den BLSV oder die DAV-Hauptverwaltung übermittelt werden, so muss dies dem Betroffenen transparent dargelegt werden, wobei auch der Zweck der Übermittlung genannt werden muss.

# Schutzbereich des Datenschutzes

- Gibt es noch weitere geschützte Daten-Bereiche, außerhalb des BDSG?

- Das Recht am eigenen Bild

Soweit abgebildete Personen nicht nur „Beiwerk“ auf dem Bild sind, dürfen Bilder, auf denen wenige identifizierbare oder benannte Personen abgebildet sind, nur mit einer Einwilligung der Abgebildeten veröffentlicht werden (gleichgültig, ob auf einer WebSite oder anderen Publikationen).

Aufnahmen aus dem Kontext von Sportveranstaltungen (Wettkämpfen) erfordern keine ausdrückliche Einwilligung. Dies gilt auch für Mannschafts-Fotos.

Bei Kindern/Jugendlichen ist eine Einwilligung der Erziehungsberechtigten erforderlich.

Keine Einwilligung ist erforderlich, wenn es sich um allgemein (auch lediglich lokal)bekannte Personen handelt (sog. relative Personen der Zeitgeschichte).

- Das Kommunikationsgeheimnis (gilt für E-Mail-, wie auch Telefon-Kommunikation) Inhalte von E-Mails oder Telefonaten dürfen nur mit Einwilligung beider Kommunikationspartner aufgezeichnet oder gar öffentlich zugänglich gemacht werden.

# Einwilligung der Betroffenen

- Wann ist eine Einwilligung der Betroffenen erforderlich?

Davon abgesehen, dass personenbezogene Daten nur mit einer ausdrücklichen Einwilligung des Betroffenen in Länder außerhalb des europäischen Wirtschaftsraumes übermittelt werden dürfen, wird für die Erhebung, Verarbeitung, Nutzung und Übermittlung personenbezogener Daten dann keine Einwilligung, wohl aber eine Information des Betroffenen benötigt, wenn:

Die Daten im Rahmen eines bestehenden Vertragsverhältnisses erforderlich sind. (z.B. die Adressdaten der Mitglieder zum Zwecke der Kommunikation Sektion/Mitglieder, oder die Bankverbindungsdaten zum Zwecke des Beitragseinzuges).

Die Daten auf der Grundlage einer gesetzlichen Regelung erhoben werden müssen oder dürfen (Diese Regelung hat beispielsweise im Mitarbeiterdatenschutz eine große Bedeutung).

Die Daten zur Wahrung eigener Interessen erforderlich sind. (z.B. beim Inkasso oder dem Versand von Vereins-/Sektions-Publikationen).

Für weitergehende Datenerhebung, Verarbeitungen, Nutzungen und Übermittlungen wird grundsätzlich eine Einwilligung benötigt.

## Einwilligung der Betroffenen

- Welche Anforderungen gelten für Einwilligungen?

Einwilligungen müssen transparent sein. D.h., der Betroffene muss erkennen können, welche Daten zu welchem Zweck erhoben und verarbeitet/genutzt werden. Darüber hinaus muss transparent werden, an welcher Stelle eventuell Daten übermittelt (weitergegeben) werden.

Einwilligungen dürfen nicht in das „Kleingedruckte“. Vielmehr sollten sie herausgehoben dargestellt werden.

Erteilte Einwilligungen müssen dokumentiert werden. Die verantwortliche Stelle ist im Streitfall beweispflichtig, dass tatsächlich eine Einwilligung gegeben wurde.

Sinnvollerweise sollten notwendige Einwilligungen, aber auch Datenschutz-Informationen, bereits in die Beitrittserklärung integriert werden. Ein Hinweis auf die Satzung, in der eine Datenschutzklausel vorhanden ist, ist nicht ausreichend.

# Einwilligung der Betroffenen

- Welche Anforderungen gelten für Einwilligungen/  
Informationen bei einer Datenerfassung über die WebSite?

Grundsätzlich ist eine Datenerhebung per WebSite nur dann zulässig, wenn vor der Absendung der erhobenen Daten, dem sog. Submit, eine Datenschutzerklärung ausgegeben wurde, in die der Datenerfasser, der Betroffene, einwilligen muss, bzw. soweit keine Einwilligung erforderlich ist, er/sie bestätigt, dass die Erklärung zur Kenntnis genommen wurde. (das sog. Opt-In)

Nach dem Opt-In ist die für die WebSite verantwortliche Stelle verpflichtet, eine sog. Begrüßungs-E-Mail an den Datenerfasser zu senden, in der ihm mitgeteilt wird, dass er seine Einwilligung gegeben hat. Darin sollte auch der Zweck, zu dem die Daten verarbeitet/genutzt werden, nochmals dargelegt werden.

Auf der Begrüßungs- und auch jeder folgenden E-Mail muss die Möglichkeit gegeben sein, der Einwilligung zu widersprechen (der sog. Unsubscribe-Link). Wird der Unsubscribe-Link betätigt, so sind die erhobenen Daten zu löschen.

## **Achtung:**

Keine Daten per Web-Site bei Kindern erheben. Kinder können nicht wirksam einwilligen.

# Transparenzpflicht

- Was bedeutet Transparenzpflicht?

Die Transparenzpflicht hat 2 Ausprägungen:

1. Betroffene müssen jederzeit wissen, wer die für die Verarbeitung/Nutzung der Daten verantwortliche Stelle ist.
2. Betroffene müssen jederzeit wissen, zu welchem Zweck die Daten erhoben, verarbeitet und genutzt, sowie eventuell an Dritte übermittelt werden.

Zu 1.

Auf der Beitrittserklärung muss transparent die verantwortliche Stelle (=Sektion/Verein) angegeben werden (dazu gehört neben den Namen auch die Vereinsregister-Nummer und die Adresse des Vereins/der Sektion, auch E-Mail-Adresse und Name des Vorstandes).

Dies gilt auch für die WebSite (hier müssen diese Angaben in das sog. Impressum) und für E-Mails (hier müssen diese Angaben in die Fußzeilen, den sog. Footer, der E-Mail).

Zu 2.

Vergleich dazu die Anmerkungen im Zusammenhang mit der Einwilligung.



# Übermittlung von Daten an Verbände

- Was ist dabei zu beachten?

Da Vereine/Sektionen rechtlich selbständig sind, ist jede Weitergabe von Mitglieder-Daten des Vereins an übergeordnete Verbände, eine Datenübermittlung.

Solche Datenübermittlungen sind nur zweckbezogen (Zweckbestimmung im Rahmen eines Vertragsverhältnisses zwischen Verband und Verein/Sektion, z.B. Verbandssatzung) zulässig.

Da in den Satzungen festgelegt ist, dass der Verband für die Vereine/Sektionen im Voraus festgelegte Aufgaben wahrnimmt, ist diese Übermittlung zulässig. Allerdings muss die verantwortliche Stelle (Verein/Sektion) die Betroffenen darüber informieren, wobei der Zweck der Übermittlung in dieser Information transparent gemacht werden muss.

Legitime Zwecke sind beispielsweise:

- ∅ Durchführung eines geregelten Wettkampfbetriebes,
- ∅ Einwerbung von Fördergeldern bei Behörden,
- ∅ Abschluss von Gruppenversicherungen oder
- ∅ Durchführung von Datensicherungen.

# Auslagerung der Datenverarbeitung an externe Dienstleister (Auftragsdatenverarbeitung)

- Was ist dabei zu beachten?

Grundsätzlich können Vereine/Sektionen externe Dienstleister mit der operativen Durchführung ihrer Datenverarbeitungsaktivitäten beauftragen. Dabei sind allerdings die im Folgenden aufgeführten Rahmenbedingungen zu beachten:

- Der beauftragte Dienstleister muss seinen Sitz und seine Betriebsstätte im Europäischen Wirtschaftsraum haben (EU-Staaten, sowie Schweiz, Liechtenstein, Norwegen und Island).
- Der beauftragte Dienstleister wird nicht zur verantwortlichen Stelle. Die Verantwortung bleibt beim Auftraggeber. Dadurch bedingt findet hier keine Datenübermittlung statt, über die die Betroffenen informiert werden müssen. Ebenso müssen keine Einwilligungen der Betroffenen eingeholt werden.
- Der Verein/die Sektion muss sich vor der Auslagerung davon überzeugen, dass beim Dienstleister ein hinreichendes Datenschutz- und Datensicherheits-Niveau gegeben ist.
- Es muss ein sog. Auftragsdatenverarbeitungs-Vertrag abgeschlossen werden, in dem:
  - Ø Die Verantwortlichkeiten der Parteien geregelt sind,
  - Ø festgelegt ist, inwiefern der Dienstleister Unterauftragnehmer einsetzen darf,
  - Ø definiert ist, welche Daten, zu welchem Zweck vom Dienstleister verarbeitet werden und
  - Ø die beim Dienstleister ergriffenen Datensicherheitsmaßnahmen definiert sind.

# Verwendung von Mitgliederdaten für Werbe-/oder Marketing-Zwecke

- Was ist dabei zu beachten?

Grundsätzlich darf der Verein/Sektion selbst erhobene Mitgliederdaten für eigene Werbe-Marketing-Maßnahmen (z.B. Versand von Informationen oder Newsletter) nutzen. Für die Verwendung von Post-Adressen, Geburtsjahr (Achtung: nicht Geburtsdatum) sowie Titel und akademische Grade wird dazu keine Einwilligung gebraucht.

Soll die Werbung aber per E-Mail versandt werden, dann braucht der Verein/die Sektion aber eine Einwilligung der Betroffenen.

Das heißt:

Selbst erhobene Adressdaten dürfen vom Verein genutzt werden, außer wenn E-Mail-Adressen oder Telefonnummern genutzt werden sollen. Dafür braucht der Verein/die Sektion eine schriftlich dokumentierte Einwilligung.

- Darf der Verein/die Sektion Adressdaten oder E-Mail-Adressen seiner Mitglieder an Werbe-Partner oder Förderer übermitteln?

Nur, wenn die Mitglieder dazu ausdrücklich ihre Einwilligung gegeben haben. Ohne Einwilligung ist dies grundsätzlich nicht zulässig.

# Datensicherheit

- Welche Datensicherheits-Maßnahmen muss der Verein/Sektion ergreifen?

Jeder Verein/Sektion, der Mitgliederdaten erhebt, verarbeitet, nutzt und an Verbände übermittelt, ist verpflichtet, Datensicherheitsmaßnahme zu ergreifen. Dazu gehört:

- Die Daten müssen so gespeichert werden, dass Unbefugte auf die Daten nicht zugreifen können (also nicht auf einem von mehreren Personen genutzten Familien-PC).
- Die Personen, die im Verein/der Sektion auf diese Daten zugreifen können, brauchen ein Login, wobei jede Person ihr eigenes Login haben sollte. Dabei sollte sichergestellt werden, dass nicht jede Person Zugriff auf alle Daten hat. Vielmehr sollte jede Person nur auf die Daten zugreifen können, die sie zur Wahrnehmung ihrer Aufgaben innerhalb des Vereins/der Sektion tatsächlich benötigt.
- Jedermann, der Zugriff auf Mitgliederdaten hat, ist auf das Datengeheimnis zu verpflichten. Diese Verpflichtung ist schriftlich zu dokumentieren.
- Jede Sektion/jeder Verein ist verpflichtet, regelmäßig die gespeicherten Daten auf einem externen Datensicherungs-Medium zu sichern (erhobene personenbezogene Daten dürfen nicht verloren gehen!).
- Die verwendeten Passwörter sollten zumindest 8 Stellen lang sein und sich aus Buchstaben (einer in Großschreibung), Ziffern und einem Sonderzeichen zusammensetzen.