Datenschutz im Verband

Hand-Out

Waltraud Meyer-Gladbach

17.09.2012

Datenschutz im Verband

Inhaltsübersicht:

1.Definitionen

- **Daten:** Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG).

- **Datenschutz:** Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten

- **Datensicherheit:** Schutz vor gespeicherten Daten vor Beeinträchtigung durch höhere Gewalt, menschliche oder technische Fehler und Missbrauch

- **Personenbezogene Daten**: Schutz vor gespeicherten Daten vor Beeinträchtigung durch höhere Gewalt, menschliche oder technische Fehler und Missbrauch

2.Basiswissen Recht/Rechtliche Aspekte

- **Personenbezogene Daten §3 Abs.9 BDSG:** sind Daten über: rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben

- **Einwilligung:** ist eine Verschärfung der Verfahrensbedingungen der Einwilligung
- Hinweis auf den Grund der Erhebung §4a,Abs. BDSG, und die Folge des Verweigerns der Einwilligung, Schriftform, soweit nicht nach dem besonderen Umständen eine andere Form angemessen(Analphabeten).Jede Einwilligung ist textlich hervorzuheben und einzeln zu unterschreiben→Pauschaleinwilligung ist rechtlich nicht zulässig
  Auch bei 13jährigen Unterschrift der Erziehungsberechtigten!

- **Verpflichtung auf das Datengeheimnis nach §5 BDSG:** Der Datenschutzbeauftragte hat die Pflicht sicherzustellen, dass alle Mitarbeiter die Vereins/Verbands, die personenbezogene Daten erheben, verarbeiten oder nutzen nachweislich zum Datenschutz und zur Geheimhaltung verpflichtet werden die einzige Methode dafür ist schriftlich und mit persönlicher Unterschrift . Eine Verweigerung ist schriftlich zu dokumentieren.

- **Recht des Betroffenen auf Auskunft (§§19, 34 BDSG)**
- Umfang der Auskunftspflicht, die jetzt Anspruchsgrundlage ist (neuer §34, Abs. 1 BDSG) zu allen zum Betroffenen gespeicherten Daten und ihre Herkunft, so fern bekannt.
- über Empfänger oder Kategorien von Empfängern
- über den Zweck der Speicherung
- Bei gewerblicher Übermittlung immer Auskunft über Herkunft (Abwägung)
- Auskunft über Daten, die zum Score geführt haben.

- **Recht des Betroffenen auf Auskunft (§§19, 34 BDSG):**

- **Zeitpunkt**: unverzüglich, d.h. im Regelfall innerhalb von ca. 2-4 Wochen

- **Form:** Auskunft muss in der Regel in Textform, Auskunftsverlangen kann formlos gestellt werden und ist grundsätzlich gratis**.**

- **Neuer §42a BDSG Information über Datenschutzverstöße**
  Verpflichtung zur Meldung binnen 48Std Selbstanzeige
  an Behörde und an Betroffenen, wenn schwerwiegende Beeinträchtigungen drohen
  Anlass: Unsachgemäße Übermittlung oder Kenntnisnahme personenbezogener Daten besonders sensibler Art (§3 Abs. 9 BDSG) z.B. Gesundheitsdaten, Berufsgeheimnisse Straftaten, Bank- oder Kreditkartenkonten

  Inhalt der Meldung
  Welche Risikodaten sind betroffen
  Wie kann der Betroffene der Schadensminderungspflicht nachkommen
  Meldung an Behörden auch mit Folgen der qualifizierten Sicherheitsverletzung und die getroffenen Gegenmaßnahmen

  Art der Meldung: (Bekanntmachung)
  per Brief oder E-Mail →$Landesdatenschutzbeauftragter\ NRW$

3. Pflichten für Vereine/Verbände

- **Grundsatz des Datenschutz**
  Vereine/Verbände sind niemals Eigentümer personenbezogener Daten, sondern nur Datentreuhänder!
  Vereine/Verbände gelten als gewerbsmäßige Betriebe

- **Aussage Datenschutzrecht**
  Datenschutz ist die aktive Wahrung der Persönlichkeitsrechte von:
  - **Mitarbeitern**
  - **Mitliedern (und deren Angehörigen)**
  - **Kooperationspartnern**
  - **etc.**

- **Wahrung der Persönlichkeitsrechte**
  Vermischen niemals von privaten Daten mit Vereinsdaten

sowie Garantie der …..

- Authentizität (Nachvollziehbarkeit der Quelle und des Verfassers)
  Sicherstellung, dass Daten tatsächlich vom Verfasser und nicht gefälscht/verändert wurden
- Revisionsfähigkeit (Prüfbarkeit)
  Die Beteiligung an einer datenbezogenen Aktion/Transaktion darf nicht zu leugnen sein.
- Transparenz (Dokumentation)
  Die einzelnen Verfahren und Aktionen/Transaktionen sind vollständig, aktuelle und nachvollziehbar zu dokumentieren

- **Datenschutzgesetze**
  - BDSG = Bundesdatenschutzgesetz→**Regel**
  - LDSG = Landesdatenschutzgesetz→**LSB/SSBK**
  - KDO/EKD = Datenschutzrecht der Kirchen→ **DJK-Vereine**

sind Auffanggesetze

Diese treten immer dann in Kraft, wenn es keine Regelungen zum Umgang mit personenbezogenen- oder personenbeziehbaren Daten gibt!

- **Verbot mit Erlaubnisvorbehalt!**
  Die Erhebung, Nutzung und Verarbeitung personenbezogener Daten ist

GRUNDSÄTZLICH VERBOTREN!

Es sei denn…..
eine Rechtsnorm erlaubt es, oder der Betroffene hat eingewilligt.

- **Beispiele Strafrecht**
  „Verletzung des persönlichen Lebens- und Geheimnisbereichs“ §§201ff StGB

- **Pflicht zur Einhaltung des Datenschutzes**
  Deutschland kennt kein Verbandsstrafrecht, weil Verbände im strafrechtlichen Sinne nicht handlungsfähig sind.
  Nach §14 StGB handelt jemand als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs oder als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft.
  die „Verantwortliche Stelle“ (§3 Abs. 7 BDSG)
  Die Geschäfts-Verbands-/Vereinsführung
  Die Mitarbeiter (auch Ehrenamtliche)
  Die Mitglieder
  Das gilt auch für Bilder/Filme (§22Kunsturhebergesetz)

Datenschutzbeauftragter DSB

Gem §4f Abs. 1 BDSG
Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben eine(n) DSB schriftlich zu bestellen.
Spätestens einen Monat nach Aufnahme der Tätigkeit
Mind. 20 Personen bei nicht automatisierter Verarbeitung
> 9 Personen bei automatisierter Verarbeitung (neu seit September 2006)

DSB – NEIN DANKE – die möglichen Folgen
Unterlassene oder unwirksame Bestellung haben negative Folgen:
Möglichkeit eines Bußgeldes (§43 BDSG) von 50.000€ bis zu 300.000€
Bußgeld auch mehrfach (für jeweiliges Zuwiderhandeln)
Verbot der Datenverarbeitung durch Aufsichtsbehörde (§38BDSG)
Meldepflicht gegenüber Aufsichtsbehörde vor jedem neuen DV-Verfahren
Schadensersatzrisiko (keine Exkulpationsmöglichkeit)

Varianten des Datenschutzbeauftragten

- Interner DSB – nebenamtlich
- Interner DSB – hauptamtlich
- Externer DSB

Die Bestellungsurkunde – inhaltliche Anforderungen

- Schriftform – Urkunde
- Aufgabenbeschreibung
- Organisatorische Stellung:
- direkt unter dem Vorstand
- Weisungsfreiheit
- Bestellungsurkunde

Stellung des betrDSB im Verein:

- Vom Vorstand bestellt und diesem unmittelbar unterstellt
- Weisungsfreiheit bei der Ausübung seiner Tätigkeit
- Unterstützungspflicht
- Keine Benachteiligung wegen seiner Tätigkeit
- Recht zur Anrufung der Aufsichtsbehörde
- Betroffene können sich jederzeit an ihn wenden

4. Datenschutz im operativen Tagesgeschäft

- **IT-Sicherheit aus Nutzersicht**
  - IT-Sicherheit ist ohne aktive Mitwirkung des Benutzers nicht möglich
  - Mitarbeiter sind die häufigste Schadensursache.
  - Verschiedene Mitarbeiter ermöglichen erst Schäden
  - Technische Schutzmaßnahmen werden häufig durch Nachlässigkeit, Unwissenheit oder Bequemlichkeit der Benutzer unwirksam.
- **Beispiele**
  - Modifikation von Datei-Endungen zur Umgehung von Virenscanner/Viruswalls
  - Installation von Software aus unsicheren Quellen
  - Nutzung von Internetzugängen auf Firmenlaptops

Einer der effektivsten Sicherheitsmaßnahmen ist die Sensibilisierung der Mitarbeiter

- **Security Awareness:** Eine Erhöhung des Sicherheitsbewußtseins im Verein/Verband erfordert eine Erhöhung des Sicherheitsbewusstseins bei den Mitarbeitern.
- Maßnahmen erfordern die aktive und positive Unterstützung der Mitarbeiter
- (Gegen-)Argumente der Anwender:
  - Arbeitsbehinderung
  - Überzogen
  - Ungeeignet

Ursache:

- Fehlende Unterstützung durch den Vorstand
- Mitarbeiter sind mit den IT-Sicherheitsrichtlinien nicht vertraut

- **Kontrollmaßnahmen gem. § 9 BDSG Anlage (zu §9 Satz 1)**
  Die Gesetzgeber haben – auf Basis des BDSG – eine Reihe von „technisch-organisatorischen Maßnahmen“ (TOM‘s) erstellt, die von allen Vereinen/Verbänden zu erfüllen sind, um die vorgeschriebene Sicherheit (Einhaltung der Sicherheitsziele) im Umgang mit Daten zu gewährleisten

  - **1.ZUTRITTSKONTROLLE**
    Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit bzw. auf denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren!! → **abschließen!**
  - **2. ZUGANGSKONTROLLE**
    Es ist zu verhindern das Datenverarbeitungssysteme von Unbefugten genutzt werden können.
  - **3. ZUGRIFFSKONTROLLE**
    Es ist zu gewährleisten, dass die Nutzung eines Daten-verarbeitungssystems, Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder

entfernt werden können!

- **4. WEITERGABEKONTROLLE**
  Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist bzw. stattgefunden hat.

- **5. EINGABEKONTROLLE**
  Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
- **6. AUFTRAGSKONTROLLE**
  Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- **7. VERFÜGBARKEITSKONTROLLE**
  Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
- **8. TRENNUNGSGEBOT**
  (Verarbeitungskontrolle)
  Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt werden können.
- **Verbandshomepage**
  Einhaltung Datenschutz zwingend erforderlich keine personenbezogene Daten weitergeben oder veröffentlichen, auch wenn die Daten-erhebung über das Internet erfolgte.
  Veröffentlichung personenbezogener Daten genehmigen lassen.
  Das gilt auch für den Newsletter und das „schwarze Brett