Datenschutz-Unterweisung

nach DSGVO

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

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

- Zum 25.05.2018 wurde das BDSG (in Verbindung mit der 95/46/EG = europäische Datenschutzrichtlinie) durch die neue DSGVO (= Europäische Datenschutzgrundverordnung) abgelöst.
- Diese DSGVO gilt direkt in den europäischen Nationalstaaten. D.h., dass das BDSG in seiner bisherigen Form durch die DSGVO abgelöst wird.
- Allerdings finden sich in der DSGVO eine Vielzahl von sog. Öffnungsklauseln. Über diese können die Nationalstaaten in einigen Sachverhalten weiterhin nationale Regeln (Gesetze), sozusagen als Ergänzung der DSGVO einführen.
- In Deutschland gibt es ein BDSG-Nachfolgegesetz (BDSG 2017), in dem die nationalen Regelungen zusammengefasst werden. Z.B. zum Beschäftigten-datenschutz oder Datenschutz in der öffentlichen Verwaltung.

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

Wichtige Aufgaben bei der Migration BDSG → DSGVO

- Die Einwilligungen der Mitglieder für die Verarbeitung und Nutzung ihrer personenbezogenen Daten müssen überarbeitet werden, wobei hier die Transparenz der Datenschutzerklärungen erhöht werden muss. Durch
  - Angabe der erhobenen personenbezogenen Attribute und
  - Zweckbezug (zu welchem Zweck werden die Daten verarbeitet)
- Die Datenschutzerklärungen für WebSites müssen zukünftig überarbeitet werden, ebenfalls mit dem Ziel, die Transparenz zu erhöhen.
- Im Bereich der Videoüberwachung müssen zukünftig alle Überwachungs-maßnahmen vorab kontrolliert und dokumentiert werden.
- Während die Auskunfts- und Korrekturrechte der Mitglieder praktisch unverändert bestehen bleiben, kommt zukünftig dem Recht auf Löschung von personenbezogenen Daten (Recht auf Vergessenwerden) eine erhöhte Bedeutung zu.

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

Wichtige Aufgaben bei der Migration BDSG → DSGVO

- Die Auftragsdatenverarbeitungsverträge, die bei der Einschaltung von Dienstleistern erforderlich sind, müssen an die Anforderungen der DSGVO angepasst werden. Wobei die „alten“ Auftragsdatenverarbeitungsverträge zumindest übergangsweise weiter gelten.
- Alle in der verantwortlichen Stelle genutzten IT-gestützten Arbeitsprozesse müssen samt den in der Sektion ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen detailliert beschrieben werden. (Verzeichnis der Verarbeitungstätigkeiten) Dazu gehört auch:
  - Ein Löschkonzept für personenbezogene Daten und
  - Eine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
- Datenschutzverletzungen sind möglichst innerhalb von 72 Stunden nach bekanntwerden an die Aufsichtsbehörde zu melden.

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

Auftragsverarbeitung:

- Auftragsverarbeitung ist nur innerhalb des EWR (plus Schweiz, Kanada, Israel) möglich.
- Sitzt Dienstleister außerhalb des EWR dann ist ein Auftragsverarbeitungsvertrag nicht möglich. Dann sind die Standard-Vertragsklauseln (Standard-Contractual-Clauses) erforderlich.
- Sonderregelung für die Verarbeitung in USA: Privacy Shield.
- Ausnahmen:
  - Banken oder Zahlungsdienstleister mit Banklizenz die der Bankenaufsicht unterliegen
  - Steuerberater / Rechtsanwälte (Kontrolle durch jeweilige Kammer)

Diese sind per definitionem keine Auftragsverarbeiter, sondern staatlich beaufsichtigte Dienstleister für die kein Auftragsverarbeitungsvertrag erforderlich ist

Datenschutz und Datensicherheit

- Grundsätzlich gilt bei der Erhebung, Speicherung, Verarbeitung und Nutzung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt, wobei zukünftig die Verarbeitung personenbezogener Daten dem Prinzip**: Treu und Glauben** unterliegt.
- Erlaubnisvorbehalte gemäß Art 6 DSGVO:
  - Gesetzliche Regelungen, die eine Erhebung, vorschreiben/erlauben.
  - Notwendigkeit der Erhebung, für eigene Geschäftszwecke.
    - Diese Geschäftszwecke müssen im Voraus definiert sein.
    - (Vor-)Vertragliches oder vertragsähnliches Verhältnis liegt vor.
    - Berechtigtes Interesse der verantwortlichen Organisation. Dabei ist das Verhältnismäßigkeits-Prinzip zu beachten (Interessenabwägung).
  - Einwilligung des Betroffenen (Art 7 DSGVO)
    - Schriftform,
    - Nachweispflicht liegt im Streitfall beim Verantwortlichen,
    - Hinweis auf Zweck und soweit
    - Daten online per Website erhoben werden doppeltes OptIn

Datenschutz und Datensicherheit

- Geschützte personenbezogene Daten sind:
  - Jede Einzelangabe über eine natürliche Person.
  - Informationen über persönliche und sachliche Verhältnisse einer natürlichen Person.
  - Achtung nach Art. 9 sind Daten über:
    - Ethnische Herkunft, politische, philosophische, religiöse Überzeugung, Gesundheit, sexuelle Orientierung sowie biometrische und genetische Daten besonders geschützt.
    - Zur Erhebung/Verarbeitung dieser Daten ist spezielle zweckbezogene Einwilligung erforderlich.
- Nicht geschützt sind:
  - Daten über juristische Personen (Unternehmen/Vereine).
  - Aggregierte Daten über Gruppen von Personen, sofern daraus keine Individuen abgeleitet werden können (Gruppe muss > 10 Personen sein).
  - Anonymisierte Daten, aus denen nicht auf Individuen geschlossen werden kann.

Datenschutz und Datensicherheit

- Erforderliche Datensicherheitsmassnahmen (für kleine Organisationen)
  - Zugangs-/Passwortschutz (Grundsätzlich personenbezogene Passwörter
  - Mindestens 8 Stellen (Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen)
  - Rollenkonzept (Regelung, wer auf welche Daten zugreifen darf)
  - Grundsatz der Datensparsamkeit
  - Server in verschlossenem Raum mit unterbrechungsfreier Stromversorgung
  - Virenscanner (Aktualisierung)
  - Regelmäßige Datensicherung mit Aufbewahrung der Sicherungsmedien in anderem Gebäude/Brandabschnitt
  - Bei Übermittlung personenbezogener Daten: End-to-End Verschlüsselung bzw. Verschlüsselung durch Zippen mit Passwort.

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

- Nutzung von Cloud-Diensten (z.B. DropBox, aber auch Amazon Drive, Microsoft Drive, Icloud, GoogleDrive, Magenta Cloud oder Secure Safe)
- Cloud-Anbieter agiert als IT-Dienstleister (Auftragsverarbeiter gemäß Art 28 DSGVO
- Soweit Cloud-Dienstleister im EWR plus (Schweiz, Kanada, Israel) ist ein AVV erforderlich
- Soweit Cloud Dienstleister in Drittstaaten, dann sind die Standardvertragsklauseln erforderlich oder bei US-Amerikanischen Dienstleistern der PrivacyShield (Achtung: Auslaufmodell)

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

- Fanpages (Facebook aber auch LinkedIn oder Xing)
  - Der Fanpagebetreiber und Facebook sind gemeinsam verantwortlich (Joint Controllership)
  - Deshalb ist eine Joint Controllership Vereinbarung (Art. 26 DSGVO) erforderlich
    - Wer (Fanpagebetreiber oder Facebook) ist für was verantwortlich
    - Wer ist Ansprechpartner für den Betroffenen
    - Wie lange werden die Daten wo gespeichert
  - Deshalb: Hinweis auf WebSite des Fanpagebetreibers auf JointControllership und Weiterleitung zur Fanpage nur nach OptIn des Besuchers (sog. 2-Schritt Zugang)
- Nutzung von Messager-Diensten (z.B.: WhatsApp)
  - Achtung: WhatsApp greift auf die Kontakte des Anwenders zu und übermittelt diese an Facebook.
  - Deshalb: WhatsApp nicht zum offiziellen Vereinsinformationsmedium machen.
  - Zulässig sind hingegen private WhatsApp-Gruppen
  - Aber: Keine personenbezogenen Daten per WhatsApp übermitteln

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

- Bilder aus dem Vereinsleben (Veranstaltungen, Ehrungen, Vereins-feiern oder Chroniken)
  - Dürfen aufgenommen und veröffentlicht werden, (mit Information dass Bilder aufgenommen werden und Bilder auf WebSite oder Vereinszeitung veröffentlicht werden)
  - Erlaubnis auf der Basis einer Interessenabwägung (Art 6 (1) lit. f) DSGVO). Argumentation: „Im allgemeinen kann man davon ausgehen, dass bei öffentlichen Veranstaltungen das Interesse des Vereines an der Darstellung in der Öffentlichkeit die Interessen der Abgebildeten übersteigt.“
  - Achtung: Bei Kindern ist für die Interessenabwägung ein gewisses Finger-spitzengefühl erforderlich.
  - Im Zweifelsfall sollte hier die Einwilligung der Erziehungsberechtigten eingeholt werden.

Datenschutz und Datensicherheit

- Gruppen-Photos (Mannschaftsaufnahmen) grundsätzlich erlaubt, da die abgebildeten bewusst posieren. (Vorherige Information besonders bei Kindern und Jugendlichen sehr sinnvoll)
- Spielscenen (Wettkampfscenen) grundsätzlich ja, soweit es sich nicht um eine Einzelaufnahme handelt. (Besonders bei Kindern und Jugendlichen ist Vorabinformation angezeigt.)
- Versand von Vereinsinformationen per E-Mail (Massen- oder Bulk-E-Mails)
  - Erlaubt, wenn die Adressaten BCC einkopiert sind
  - Ansonsten: Datenschutzverletzung durch Offenlegung von E-Mail-Adressen
  - Achtung: Keine personenbezogenen Daten per E-Mail versenden außer:
    - End-to-End Verschlüsselung einsetzen oder
    - Daten liegen in verschlüsselten Attachements

Datenschutz und Datensicherheit

- **Rechte der Betroffenen:**
  - Benachrichtigung bei Datenerhebung ohne Kenntnis des Betroffenen. (Siehe oben)
  - Auskunftsrecht des Betroffenen
    - Welche personenbezogene Daten sind gespeichert und für welchen Zeitraum.
    - Zu welchem Zweck werden die Daten verarbeitet und gespeichert
    - An welchen Dritten werden sie evtl. übermittelt. (Achtung: Auftragsverarbeiter ist kein Dritter.)
  - Recht auf Vergessenwerden bei Websites (Digitaler Radiergummi).
  - Berichtigung, Sperrung und Löschung
    - Berichtigung bei nachweislich fehlerhaften Daten
    - Sperrung, wenn Zweck der Speicherung weggefallen ist und eine Löschung gemäß anderen gesetzlichen Vorgaben (HGB, AO oder sonstiger Rechtsgrundlage) nicht möglich ist (Einschränkung der Verarbeitung).
    - Löschung, wenn Erhebung der Daten unzulässig war oder auf Antrag (Recht auf Vergessenwerden) soweit Löschung überhaupt zulässig.

Datenschutz und Datensicherheit

- **Datenschutzkonforme Organisation:**
  - Dokumentationspflicht / Vorlagepflicht auf Verlangen der Aufsichtsbehörde.
  - Verfahrensverzeichnis aller Anwendungen (Verarbeitungsvorgänge).
  - Risikobewertungen für kritische Verfahren (z.B. bei Verarbeitung von Daten nach Art 9 DSGVO oder bei Big-Data-Anwendungen).
  - Datenschutzfolgeabschätzungen durch Einführung von Schutzklassen, denen die Verfahren zugeordnet werden.
  - Einsatz datenschutzfreundlicher Technologien (Verschlüsselung, Anonymisierung/ Pseudonymisierung, Löschkonzepte).
  - Anwendung datenschutzfreundlicher Voreinstellungen bei Verfahren. (Z.B. keine Voreinstellungen bezüglich Einwilligungen auf Web-Sites)
  - Einsatz technischer und organisatorischer Maßnahmen zum Datenschutz/Datensicherheit gemäß dem jeweils aktuellen Stand der Technik.

(c) 2018 Prof. Dr. Rolf Lauser

Datenschutz und Datensicherheit

- **Für den einzelnen Mitarbeiter bedeutet Datenschutz:**
  - Personenbezogene Daten dürfen nur zur Erfüllung der Übertragenen Aufgaben erhoben, gespeichert, verarbeitet oder genutzt werden.
  - Im Unternehmen dürfen nur solche Mitarbeiter mit der Erhebung, Verarbeitung, oder Nutzung personenbezogener Daten betraut werden, die auf das Datengeheimnis verpflichtet sind.
  - Personenbezogene Daten sind grundsätzlich, auch innerhalb der Organisation vertraulich zu behandeln.
  - Zugangsdaten (Passwörter) müssen geheim gehalten werden.
  - Personenbezogene Daten dürfen nur dann an andere Stellen (innerhalb der Organisation oder an andere Organisationen (auch innerhalb des gleichen Konzerns) weitergegeben werden, wenn ein Erlaubnisvorbehalt vorliegt, der Zweckbezug dies zulässt und ein Auftragsverarbeitungsvertrag vorliegt.
  - Die Verpflichtung auf das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.