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

Datenschutz und Datensicherheit

- Zum 25.05.2018 wird das BDSG (in Verbindung mit der 95/46/EG = europäische Datenschutzrichtlinie) durch die neue DSGVO (= Europäische Datenschutzgrundverordnung) abgelöst.
- Diese DSGVO gilt dann 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, in dem die nationalen Regelungen zusammengefasst werden. Z.B. zum Beschäftigtendatenschutz.
- Achtung: Regelungen des TMG und des UWG bleiben unverändert bestehen.

Datenschutz und Datensicherheit

- Wichtige nationale Regelungen betreffen, neben dem Datenschutz im Bereich der öffentlichen Verwaltung:
  - Den betrieblichen Datenschutzbeauftragten, der in Deutschland mit erweitertem Aufgabenspektrum beibehalten wird und
  - der Beschäftigtendatenschutz (§ 32 BDSG), der unverändert bleiben wird. Allerdings steht zu erwarten, dass er zukünftig in Deutschland erweitert werden wird.
- Ansonsten wird die DSGVO einige Verschärfungen der Datenschutzvorschriften bringen. Beispielsweise bezüglich:
  - Der Anforderungen an die Einwilligungen,
  - der Anforderungen an die Datenschutzorganisation (Dokumentation),
  - der Höhe der Bußgelder und
  - der Datenschutzerklärungen
- Der § 6b BDSG (Videoüberwachung) fällt zukünftig weg. D.h. jede Videoüberwachung muss zukünftig dokumentiert werden.

Datenschutz und Datensicherheit

- Eine wichtige Änderung betrifft die Nutzung von Adressdaten für Werbe- und Marketingzwecke:
  - Das sog. Listprivileg fällt weg. Damit gelten zukünftig auch für die Nutzung von Post-Adressen (Werbebriefe) die identischen Vorgaben wie für E-Mail- und Telephonwerbung.
  - D.h., auch für Werbe- und Marketing-Briefe werden zukünftig Einwilligungen erforderlich.
  - Die „alte“ Widerspruchslösung, anstelle einer Einwilligung, wird gekippt.
- Daraus folgt:
  - Datenschutzerklärungen müssen erweitert werden (Online und Offline).
  - Die Durchführung von Werbe-Kampagnen muss zentral grundsätzlich überdacht werden, evtl. durch
    - eine nachträgliche Einholung von Einwilligungen der Betroffenen

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

- Zur Durchsetzung des Schutzes der personenbezogenen Daten basiert die DSGVO, neben dem **Grundsatz der Datenminimierung (Art. 5 (1) lit. c,** auf den 7 Grundregeln:
  - Rechtmäßigkeit der Verarbeitung (Art. 6 evtl. in Verbindung mit Art.7),
  - Transparenz (Art. 12 bis 14, sowie 19 und 34),
  - Rechte der Betroffenen (Art. 15 bis 21),
  - Kontrolle (Art. 37 bis 39 (DSB) und Art. 57 und 58 (Aufsichtsbehörden),
  - Sanktionen (Art. 82 und 83),
  - Datenschutzkonforme Organisation (Art. 24 bis 32 und 35 bis 36) und
  - Nationale Öffnungsklauseln.

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

- **Transparenz:**
  - Die Erhebung und Verarbeitung personenbezogener Daten durch den Verantwortlichen darf nicht „hinter dem Rücken“ des Betroffenen stattfinden.
  - Schriftliche Information (Datenschutzerklärung) online und offline, aus der Umfang der Datenerhebung, Zweck der Verarbeitung und Speicherdauer der Daten hervorgehen.
  - Hinweis auf Rechte des Betroffenen (Auskunft, Korrektur, Sperren/Löschen und Widerspruchsrecht)
  - Datenerhebung grundsätzlich beim Betroffenen. Wenn Datenerhebung bei Dritten, dann Information des Betroffenen über die Datenerhebung.
  - Information über den Verantwortlichen (Impressum).
  - Information über in die Verarbeitung eingeschaltete Dritte (Sitzt Dritter außerhalb des Gültigkeitsbereiches der DSGVO, dann ist Einwilligung erforderlich).
  - Gemeinsame Verantwortung (Joint Controller) z.B. im Zusammenhang mit Franchisepartnern, in Konzernen oder im Verhältnis Verband/Verein möglich.

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 die verarbeitet und gespeichert werden.
    - An welchen Dritten werden sie 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) 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

- **Kontrolle:**
  - Intern: der betriebliche DSB
  - Extern: die jeweils zuständige Aufsichtsbehörde
  - Wobei: Konzerne können für eine Aufsichtsbehörde optieren
  - Achtung: Verbraucherverbände

- **Sanktionen:**
  - Bussgeldrahmen wurde wesentlich (drastisch) erhöht.
  - Bis € 20 Mio bzw. 4% des weltweiten Umsatzes.
  - Bei Auftragsdatenverarbeitung: auch Dienstleister haftet.
  - D.h. Nicht nur der Auftraggeber muss den Dienstleister überwachen, sondern der Dienstleister muss auch den Auftraggeber auf evtl. Datenschutzverstöße hinweisen.

Datenschutz und Datensicherheit

- **Datenschutzkonforme Organisation:**
  - Dokumentationspflicht / Vorlagepflicht auf Verlangen der Aufsichtsbehörde.
  - Dokumentierte Datenschutz-Policy / Strategie erforderlich.
  - 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, physikalische 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.

Datenschutz und Datensicherheit

- **Speziell bei Sales & Marketing ist zu beachten:**
  - Telephonwerbung (Cold-Calls) sind nach § 7 Abs. 2 Punkt 2 UWG grundsätzlich verboten, außer es liegt eine dokumentierte Einwilligung vor.
  - E-Mail-Werbung (auch Newsletter) sind nach § 7 Abs. 2 Punkt 3 UWG auch nur mit einer dokumentierten Einwilligung zulässig.
  - Liegen für Telephon- und E-Mail-Werbung keine Einwilligungen vor, dann besteht eine latente Abmahnungsgefahr gegen die verantwortliche Stelle.
  - Listenprivileg für postalische Werbung fällt weg.
  - Wenn Adressen für Werbe-Post zugekauft / gemietet werden sollen, dann müssen dokumentierte Einwilligungen der Betroffenen vorliegen.
  - Identisches gilt für Verkauf / Vermietung von Adressen.
  - Verantwortliche Stelle muss Herkunft der Adressen dokumentieren.
- TMG und UWG bleiben weiterhin bestehen. (werden nicht durch DSGVO abgelöst)

Datenschutz und Datensicherheit

- **Vorgehen bei postalischer- oder E-Mail-Werbung:**
  - Einholung der Einwilligung des Betroffenen bereits bei der Datenerhebung.
  - Bei Adressensammlung über Web-Site geschieht dies nach § 13 TMG.
    - Ausgabe einer Datenschutzerklärung.
    - Zwangs-Opt-In (mit Protokollierung).
    - Erst nach dem Opt-In dürfen erhobene Daten submitted werden.
  - Falls Werbung per „gelbe“ Post:
    - In jedem Brief muss auf Widerspruchsmöglichkeit hingewiesen werden
  - Falls Werbung per E-Mail:
    - Erste Mail = Begrüßungs-Mail (Wenn möglich ohne Werbung, höchstens Links zu Werbung). Erst wenn hier kein Widerspruch erfolgt liegt die Einwilligung vor
    - Auf jeder E-Mail muss Unsubscribe-Link vorhanden sein
  - D.h. Einwilligung gilt nur von Brief zu Brief / E-Mail zu E-Mail
  - Keine dauerhafte Einwilligung möglich
  - Grundsätzlich besteht eine Impressumpflicht.

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, ..., 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 oder der Zweckbezug dies zulässt.
  - Die Verpflichtung auf das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.