LANSKY, GANZGER + partner

LGP RECHTSANWÄLTE / ATTORNEYS

DSGVO in der Praxis

Eine Präsentation für das Bundesgremium des Foto-, Optik- und Medizinproduktehandels der WKO Österreich

Wien, am 26.02.2018

RAA Ing. Mag. Amra Bajraktarevic

Problemstellung

- Welche Daten der betroffenen Person werden
- zu welchem Zweck
- auf welcher Rechtsgrundlage erhoben und
- an wen werden diese weitergegeben?

Welche Rechtsgrundlage (Art 6)?

Jede Datenanwendung erfordert eine Rechtsgrundlage. Für Gesundheitsunternehmen sind die betreffenden Rechtsgrundlagen nach Art 6 DSGVO folgende:

- Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung
- (Überwiegende) berechtigte Interessen des Verantwortlichen
- Vorliegen einer Einwilligung
- Vorliegen einer rechtlichen Verpflichtung

Rechtsgrund Vertragserfüllung (Art 6)

- Soweit Kundendaten verarbeitet werden, die für die Vertragserfüllung erforderlich sind, ist keine Zustimmung notwendig
- Trifft auch auf Durchführung vorvertraglicher Maßnahmen (zB Terminvereinbarung, Einholung eines Angebotes) zu
- Trifft auf Datenverarbeitung zu Marketingzwecken regelmäßig nicht zu

Rechtsgrund berechtigte Interessen I (Art 6)

- Hinreichend konkretes und berechtigtes Interesse des Verantwortlichen oder eines Dritten
- Die verfolgten Ziele sind rechtmäßig und stehen im Einklang mit der Rechtsordnung
- Interessenabwägung schlägt im Einzelfall zu Gunsten des Verantwortlichen aus

Rechtsgrund berechtigte Interessen II

- Als berechtigte Interessen anerkannt:
  - Übermittlung von personenbezogenen Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten (Erwägungsgrund 48)
  - Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung (Erwägungsgrund 47)
- Interessenabwägung durchführen und dokumentieren!
- Informationspflicht beachten!

Rechtsgrund Einwilligung I

- Bedingungen für die Einwilligung:
  - Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in klarer und einfacher Sprache
  - Einwilligung erfolgt freiwillig, für den bestimmten Fall, in informierter Weise
  - Keine Kopplung an die Erbringung der Leistung
  - Erkennbare Trennung vom übrigen Sachverhalt
  - Hinweis auf das Widerrufsrecht

Rechtsgrund Einwilligung I – Beispiel Kopplungsverbot

LANSKY, GANZGER partner
LGP RECHTSANWÄLTE/ATTORNEYS

□ Ich habe die AGB sowie die Datenschutzbestimmung der XXX GmbH gelesen und akzeptiere diese.(1)

1) Wir nutzen Ihre Daten auch, um Sie über unsere Produkte und Dienstleistungen sowie relevante Neuigkeiten per E-Mail zu informieren. Sie können einer Verarbeitung oder Nutzung Ihrer Daten jederzeit schriftlich oder per E-Mail an office@XXX.at widersprechen.

Rechtsgrund Einwilligung II

- Bedingungen für die Einwilligung:
  - Einwilligung setzt eindeutig bestätigende Handlung voraus:
    - Schriftlich, mündlich, elektronisch, Anklicken von Checkboxen
    - NICHT: Stillschweigen, Untätigkeit, Vorangekreuzte Checkboxen
  - Inhalt einer Erklärung:
    - Welche personenbezogenen Daten werden zu welchem Zweck verarbeitet
    - Wer darf die Daten konkret nutzen, an wen dürfen die Daten weitergegeben werden
    - Allenfalls: Wie lange dauert die Nutzung an

Formulierungsvorschlag Einwilligung

- Beispielhafter Formulierungsvorschlag:

„Ich stimme zu, dass meine personenbezogenen Daten, nämlich … [konkrete Aufzählung der Datenarten, z.B. Name, Adresse, etc] zum Zweck der … [konkrete Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma …“] bei der Firma [Firmenname] gespeichert werden. Diese Einwilligung kann jederzeit bei … [Kontaktdaten] widerrufen werden.“

Fälle: Direktmarketing

- Bei elektronischer Kommunikation ist weiterhin § 107 TKG zu beachten:
- Werbeanrufe: Einwilligung erforderlich (§ 107 Abs 1 TKG)
- E-Mail-Werbung an „Nicht-Kunden“: Einwilligung erforderlich (§ 107 Abs 2 TKG; Zweckbindungsgrundsatz beachten!)
- E-Mail-Werbung an Kunden: gs keine gesonderte Einwilligung erforderlich, allerdings zu beachten:
  - Erlaubt ist Direktmarketing für eigene, ähnliche Produkte
  - Unbedingtes Widerspruchsrecht des Kunden (Opt-Out bei Datenerhebung und bei jeder Zusendung)
  - Eintragungen in Robinson-Liste (bei RTR) beachten

Sensible Daten (Art 9)

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse und weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- **Genetische Daten** (Art 4 Z 13)
- **Biometrische Daten**, die zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden (Art 4 Z 14)
- **Gesundheitsdaten** (Daten über die körperliche und geistige Gesundheit, einschließlich der Erbringung von Gesundheitsdienst-leistungen Art 4 Z 15)
- Daten zum Sexualleben oder zur sexuellen Orientierung

Welche Rechtsgrundlage (Art 9)?

Bei der Verarbeitung sensibler Daten kommen folgende Rechtsgrundlagen in Frage (Art 9 Abs 2 DSGVO):

- Vorliegen einer ausdrücklichen Einwilligung (lit a)
- Erfüllung einer rechtlichen Verpflichtung aus dem Arbeitsrecht, Recht der sozialen Sicherheit und des Sozialschutzes (lit b)
- Schutz lebenswichtiger Interessen (lit c)
- Erhebliche öffentliche Interessen (lit g)
- Gesundheitsvorsorge und Arbeitsmedizin, medizinische Diagnostik, Versorgung und Behandlung im Gesundheits- oder Sozialbereich (lit h) – Geheimhaltungspflicht!
- Öffentliche Interessen im Bereich der öffentlichen Gesundheit (lit i)

Rechtsgrundlage: Gesetzliche Bestimmung

Folgende gesetzlichen Bestimmungen kommen für die Verarbeitung zB in Frage:

- § 51 ÄrzteG / § 10 KAKuG bzw landesrechtliche KAG
- § 110a MPG
- §§ 73f MPG
- § 11a ff VersVG

Welche Empfänger?

- Weitergabe personenbezogener Daten erfolgt idR an
  - Behandelnde/zuweisende Ärzte bzw Krankenanstalten
  - Verrechnungsstellen
  - Versicherungsträger
  - Lohnverrechner
  - aber auch an IT-Unternehmen, ua

Datenweitergabe zu Zwecken der Auftragsverarbeitung

- Rechtsgrundlage gs: schriftlicher / elektronischer Vertrag mit folgendem Inhalt:
  - Gegenstand und Dauer der Verarbeitung
  - Art und Zweck der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Hinzuziehung Sub-Auftragsverarbeiter nur mit Genehmigung
  - Pflichten und Rechte des Verantwortlichen
- Auftragsverarbeiter ergreift technische und organisatorische Maßnahmen (insb nach Art 32 DSGVO), um Anforderungen der DSGVO zu entsprechen
- Personenbezogenen Daten werden nach Abschluss der Tätigkeit zurückgestellt oder gelöscht

Informationspflichten (Art 13f DSGVO)

- Verantwortliche sind verpflichtetet, Betroffene bei der Datenerhebung über die Datenverarbeitungsvorgänge zu informieren.
- Information hat zu enthalten:
  - Namen und Kontaktdaten des Verantwortlichen
  - Zwecke und Rechtsgrundlagen der Datenverarbeitung
  - Empfänger / Kategorien von Empfängern der personenbezogenen Daten
  - Speicherdauer
  - Information über Betroffenenrechte
  - Information über Beschwerderecht bei der Aufsichtsbehörde

Verfahrensverzeichnis 1

- Anstatt des bisherigen Datenverarbeitungsregisters kommt das „Verfahrensverzeichnis“ (Art 30 DSGVO).
- Ausnahme: Die Vorschriften des Art 30 Abs 1 und 2 DSGVO gelten nicht für Unternehmen mit weniger als 250 Mitarbeitern, sofern die von ihnen vorgenommen Verarbeitung nicht
  - ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt und die Datenverarbeitung nur gelegentlich erfolgt und
  - nicht die Verarbeitung besonders sensibler Daten oder über strafrechtliche Verurteilungen und Strafdaten einschließt.
- Ist auf Anfrage der Aufsichtsbehörde vorzulegen

Verfahrensverzeichnis 2

- Das Verfahrensverzeichnis hat **folgende Informationen** zu enthalten:
  - die eigenen Kontaktdaten;
  - die Zwecke der Datenverwendung;
  - eine Beschreibung der in der Datenanwendung enthaltenen Datenkategorien;
  - eine Beschreibung der in der Datenanwendung enthaltenen Empfängerkategorien;
  - Datentransfers in Drittstaaten (separat ausgewiesen);
  - **NEU**: die geplante Speicherdauer (wenn möglich);
  - eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

Datenschutz-Folgenabschätzung 1

- Datenschutz-Folgenabschätzung ist erforderlich, wenn eine Datenverarbeitung
  - mit **neuen Technologien** arbeiten und
  - im Hinblick auf ihre Art, Anwendungsbereich, Kontext und Zwecke möglicherweise ein **hohes Risiko** für die Privatsphäre der Betroffenen beinhaltet
- Unabhängig von der Unternehmensgröße
- Anwendungsfälle:
  - Systematische und extensive Auswertung von persönlichen Aspekten (insb. durch „Profiling“)
  - Verarbeitung von sensiblen Daten oder
  - Verarbeitung von strafrechtlich relevanten Daten
- Bei hohem Risiko ist Vorab-Konsultation mit der Datenschutzbehörde durchzuführen

Datenschutz-Folgenabschätzung 2

- Inhalt einer Datenschutzfolgenabschätzung:
  - **Beschreibung** der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung
  - Bewertung der **Notwendigkeit und Verhältnismäßigkeit** der Verarbeitungsvorgänge in Bezug auf den Zweck
  - Bewertung der **Risiken** für die Rechte und Freiheiten der betroffenen Personen und
  - Zur Bewältigung der Risiken geplante **Abhilfemaßnahmen**

Formularmuster

Muster: https://www.wko.at/branchen/handel/D_04a-Verfahrensverzeichnis.xlsx

Rechnungswesen und Geschäftsführung

VT01 (SA001)

- Buchhaltung bzw Einnahmen-Ausgaben-Rechnung
- Verarbeitungen im Rahmen des Steuerrechts bzw Übermittlungen an Steuerberater und Finanzamt
- UVAs
- Kostenrechnung
- Verwaltung der Bankkonten bei Kreditinstituten (Zahlungsverkehr)
- Auflagen iZm Registrierkassen
- Ausgangs- und Eingangsrechnungen (Einkauf / Verkauf)
- Miet- und Leasingverträge
- Versicherungen
- Lagerverwaltung (incl Inventurunterlagen)
- ....

Sicherheitsmaßnahmen

Geeignete technische und organisatorische Maßnahmen sind zB:

- präventive: Pseudonymisierung und Verschlüsselung personenbezogener Daten, Anti-Viren-Software
- detektive: Sicherstellung Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme durch netzwerkbasierte Einbruchserkennungssysteme
- reaktive: Implementierung Systeme zur Wiederherstellung der Verfügbarkeit zu Daten und System nach Zwischenfällen (zB Backups)
- organisatorische: Mitarbeiterschulungen
- physische: Zutrittssysteme

Datenschutz durch Technik

- Zwei Gruppen von (technischen und organisatorischen) Maßnahmen:
  - **Privacy by Design** (Gestaltung der Datenverarbeitung)
  - **Privacy by Default** (datenschutzrechtliche Voreinstellung)
- Nachweis durch **Zertifizierungsverfahren** (Art 42 f DSGVO)

Datenschutz zur Technikgestaltung – Privacy by Design

- Maßnahmen / Mittel zur Umsetzung des Datenschutzes durch Technik

- Technische und organisatorische Maßnahmen, zB:
  - **Pseudonymisierung**;
  - Umsetzung der **Datenschutzprinzipien**, zB
    - Datenminimierung und
    - Einbau von Datensicherheitsmaßnahmen

Datenschutz durch Technikgestaltung – Privacy by Default

- Pflicht zu datenschutzfreundlichen Voreinstellungen

- Sicherstellung, dass
  - grundsätzlich **nur** personenbezogene Daten, deren Verarbeitung **für** den jeweiligen **bestimmten Verarbeitungszweck erforderlich sind**, verarbeitet werden
  - Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden

- Diese Verpflichtung gilt für
  - die Menge der erhobenen personenbezogenen Daten
  - den Umfang ihrer Verarbeitung
  - ihre Speicherfrist und
  - ihre Zugänglichkeit

Ihre Vortragende

RAA Ing. Mag. Amra BAJRAKTAREVIC

- HTL-Absolventin (Schwerpunkt EDV & Organisation) und mehrjährige Erfahrung als Netzwerkadministratorin
- Seit 2011 als Rechtsanwaltsanwärterin bei LGP
- Studentin des postgraduate Lehrgangs „Informations- und Medienrecht“
- Schwerpunkte: Zivil- und Zivilprozessrecht, IT/IP-sowie Datenschutzrecht und Kartellrecht
- Autorin für Magazine des Manstein Verlags sowie Austria Innovativ

Kontakt

Ing. Mag. Amra Bajraktarevic

Lansky, Ganzger & Partner
Rechtsanwälte GmbH

Biberstraße 5
1010 Wien

T: +43 1 533 33 30
E: bajraktarevic@lansky.at
W: www.lansky.at