EU-Datenschutzgrundverordnung & Marktforschung

VMÖ
Wien, 09.04.2018

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e.V.

EU-Datenschutzgrundverordnung (EU-DSGVO)

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

- wird nach 2jähriger Übergangsfrist am 25.05.2018 wirksam
- gilt als Verordnung unmittelbar
- wird ggf. ergänzt durch nationale Datenschutzgesetze
- gilt für personenbezogene Datenverarbeitung in Unternehmen und Behörden
- gilt in der EU und außerhalb, wenn Daten von Unionsbürgern verarbeitet werden
- enthält für Datenverarbeiter Informations-, Dokumentations- und Organisationspflichten
- enthält aufgefächerte Betroffenenrechte

Nationale Datenschutzgesetze

- Österreich: Datenschutz-Anpassungsgesetz 2018

https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig

- Deutschland: Datenschutz-Anpassungs- und Umsetzungsgesetz

https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1520093154412

Informations-, Dokumentations-, Organisationspflichten

- Datenschutzerklärung mit Rechtebelehrung
- Verfahrensverzeichnis
- Auftragsverarbeitervereinbarungen
- Information bei Datenschutzvorkommnis: an Betroffenen und an Aufsicht
- ? Datenschutzfolgenabschätzung: bei sensiblen Daten
- ? Datenschutzbeauftragter: bei Behörden, Unternehmen ab 250 MA (in DE ab 9) oder wenn Verarbeitung sensibler personenbezogener Daten; bei Verzicht Gründe dokumentieren

Betroffenenrechte

- Information bei Datenerhebung
- Auskunft
- Berichtigung
- Löschung (erweitert: "Vergessenwerden")
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch

Auskunft

- Kategorien und Inhalte der Daten, die verarbeitet werden
- Rechtsgrundlage
- Verarbeitungszwecke
- Datenempfänger (wer, wo, wozu)
- bei Drittstaatenübermittlung: Sicherheitsgarantien
- Auftragsverarbeiter
- bei Entscheidungen, die auf automatisierter Verarbeitung beruhen - einschließlich Profiling - und gegenüber der betroffenen Person rechtliche Wirkungen entfalten: Angaben zur verwendeten Logik und zu den Auswirkungen

Datenschutzerklärung

Gut auffindbar, einfache Sprache

Mindestangaben:
– Kontaktdaten des Unternehmens als verantwortliche Stelle
– alle Zwecke, zu denen personenbezogene Daten verarbeitet werden
– Rechtsgrundlagen für die Datenverarbeitung
– Speicherfristen
– Katalog der Betroffenenrechte gemäß DSGVO
– Kontaktdaten der zuständigen Aufsichtsbehörde für Anfragen und Beschwerden

Einzelfallbezogene Informationspflichten in Abhängigkeit von den tatsächlichen Gegebenheiten:
– Kontaktdaten des Datenschutzbeauftragten, sofern einer bestellt ist
– berechtigte Interessen, die mit der Datenverarbeitung verfolgt werden
– Empfänger (Dritte), an die erhobene Daten übermittelt werden
– Absicht, die Daten ins Nicht-EU-Ausland zu übertragen und der diesbzügliche Rechtsrahmen
– ggf. Verpflichtung zur Bereitstellung der Daten seitens des Betroffenen und Folgen der Nichtbereitstellung
– Einsatz von automatisierten Entscheidungsfindungen, wenn praktiziert
– Einsatz von Tools zur Webseitennutzungsanalyse und deren Funktionsweise bzw. Art der Datenerhebung und -verarbeitung
– Einsatz von Cookies und deren Art, Umfang und Zweck
– Social-Media-Applikationen und deren Art und Zweck, sowie die sich aus der Nutzung für den Betroffenen ergebenden technisch-rechtlichen Implikationen, z.B. Datenübermittlung an den Social Media Provider

Hinweis: Diese Angaben sind nicht abschließend. Es gibt keine für alle Konstellationen einheitlich gültige oder anwendbare Datenschutzerklärung, sondern diese muss auf die tatsächlichen Verhältnisse angepasst sein. Die Erklärung muss in verständlicher Sprache, d.h. nicht in juristischem oder IT-Kauderwelsch verfasst sein und sollte eine sinnvolle Länge nicht überschreiten. Sofern auf längere Erläuterungen nicht verzichtet werden kann, bietet sich eine Kurzversion mit "anklickbaren" Textfenstern für nähere Ausführungen an.

Verarbeitungsverzeichnis

(nicht verallgemeinerbares Beispiel)

Nr.	Bezeichnung der Anwendung bzw. des IT-Verfahrens	Eingesetzte IT	Eingesetzte Software	Zweck-bestimmung	Daten-Kategorien	Betroffenen-Kategorien	Empfänger-Kategorien	Rechts-grundlage	Übermittlung an Drittstaaten	Auftrags-verarbeitungs-vertrag	Löschfrist/ Speicherdauer	Zugriffsbe-rechtigte Personen	DSFA: Risiko für Betroffene (Zuordnung Risikoklasse siehe Erläuterungen)	*Risiko für Verantwortliche (Zuordnung Risikoklasse siehe Erläuterungen)*	Technisch-organisato-rische Maßnahmen

Technisch-organisatorische Maßnahmen

Ansatz: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

"privacy by design" / "privacy by default"

- Datenhaltung (Sicherung)
- Kommunikation (Verschlüsselung?)
- Management (Verantwortlichkeiten)
- Zutrittskontrolle (wer kommt hinein)
- Zugangskontrolle (wer nutzt)
- Zugriffskontrolle (wer greift auf was zu)
- Weitergabekontrolle (an wen)
- Eingabekontrolle (durch wen)
- Auftragskontrolle
- Verfügbarkeitskontrolle (physischer Schutz)
- ggf. getrennte Verarbeitung (Zweck)

Datenübermittlung in Drittländer

- "Geeignete Garantien“
- "Privacy Shield" (USA)
- "Corporate Binding Rules"
- Standardvertrag

Newsletter

Rechtliche Maßgaben

Bei bestehender Geschäftsbeziehung:

Altkunden: Bisheriger Versand kann fortgesetzt werden, wenn im Rahmen der Zweckbestimmung der bisherigen Geschäftsbeziehung, und nicht widersprochen wurde, nachträgliche Einwilligungseinholung ist gleichwohl empfehlenswert (wenn praktikabel)

Neukunden: Mit Einwilligung
- mit doppelter Bestätigung ("Double opt-in")
- Einwilligung darf nicht versteckt, voraktiviert oder an eine Leistungserbringung gekoppelt sein

Newsletter-Versendung muss regelmäßig erfolgen, andernfalls "erlischt" die Einwilligung (mindestens ein- bis zweimal jährlich)

Bei keiner bestehenden Geschäftsbeziehung:
- sofern keine ausdrückliche Einwilligung vorliegt, Betrachtung analog zu Direktmarketing, d.h. Interessenabwägung zwischen berechtigtem Interesse des Versenders und des Betroffenen
- Nachweis der vorgenommenen Interessenabwägung
- datenschutzrechtliche und wettbewerbsrechtliche Grauzone

Technische Maßgaben

Newsletterfunktionalität auf Webseite (Eintragungsmöglichkeit)
- mit doppelter Bestätigung ("Double opt-in")
- Einwilligung darf nicht versteckt, voraktiviert oder an eine Leistungserbringung gekoppelt sein
- empfehlenswert: Protokollierung des Zeitpunktes

Bei Versand über Dienstleister, z.B. Web-Applikationen
- wenn Dienstleister in der EU ansässig, dann = Auftragsverarbeitung i.S.d. DSGVO
- wenn nicht in der EU ansässig, dann "EU-Standardvertrag" notwendig
- wenn z.B. in den USA ansässig, dann "Privacy Shield"-Anwendung

- Abbestellmöglichkeit (Mailkontakt, Link)
- Tracking des Leseverhaltens (z.B. Tracking Pixel, die beim Öffnen nachgeladen werden) nur mit vorheriger Einwilligung
- Problem: bei einigen Newsletter-Programme muss Tracking vom Versender deaktiviert werden, manche Programme ermöglichen keine Deaktivierung
- Newsletter-Funktionalität muss mit Sicherheitszertifikat gesichert sein

Markt-, Meinungs- und Sozialforschung

Besonderheiten:

- Erhebung einer Vielzahl personenbezogener Daten bei identifizierbaren Personen, auch sensible Daten
- deshalb: Erhöhte Anforderungen im Datenschutzrecht sowie berufsständische Verhaltensregeln (VMÖ, ADM, BVM, Esomar) + ISO 20252
- basiert auf wissenschaftlich-methodischem Vorgehen
- trifft keine Aussage über Einzelpersonen, sondern zum Verhalten von Gesellschaftsgruppen
- ist anonym - Personenbezogene Daten der Teilnehmer werden nicht an den Auftraggeber weitergegeben.
- muss Daten so schnell wie möglich pseudonymisieren
- unterliegt strengem Zweckbindungsgrundsatz: bei Marktforschung gewonnene personenbezogene Daten dürfen nicht zu Werbe- und Marketingzwecken verwendet werden.

Markt-, Meinungs- und Sozialforschung

Bisher:

- auf Basis einer Einwilligung oder auf Rechtsgrundlage zulässig
- Einwilligung als Grundlage nicht immer ausreichend, da sie Teilnehmerkreis auf Personen beschränkt, zu denen bereits Kontakt bestand und die zuvor eingewilligt haben.

Beispiel DE (§ 30a BDSG):

Marktforschung auch ohne Einwilligung zulässig, wenn kein Grund zur Annahme, dass Betroffener schutzwürdiges Interesse am Ausschluss der Erhebung, Verarbeitung, Nutzung hat oder die personenbezogenen Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle die Daten ohnehin veröffentlichen dürfte; Berufliche Verhaltensregelungen und ISO-Normen teilweise strenger

Markt-, Meinungs- und Sozialforschung

Jetzt:

- in DSGVO keine vergleichbare Spezialnorm
- Erlaubnistatbestände, Pseudonymisierung, Anonymisierung, Zweckbindung für Marktforschung nicht explizit geregelt
- deshalb: Marktforschungsprojekte künftig nach den allgemeinen Grundsätzen der DSGVO

Erlaubnistatbestände:

Beispiele:
- Einwilligung (Art. 6 Abs. 1 Lit. a DSGVO)

oder

- berechtigtes Interesse des Auftraggebers (Art. 6 Abs. 1 Lit. f DSGVO)

Markt-, Meinungs- und Sozialforschung

Wichtig:

Marktforschung = wissenschaftliche Forschung i.S.d. Art. 89 Abs. 1 DSGVO

dadurch Privilegien:

- Daten könnten für Sekundärzwecke genutzt werden (Art. 5 Lit. b DSGVO)
  Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken

- Daten können auch nach Zweckerreichung gespeichert werden (Art. 5 Lit. e DSGVO)
  Personenbezogene Daten dürfen länger gespeichert werden, soweit sie vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden

- Von Betroffenenrechten können Ausnahmen gemacht werden (Art. 89 Abs. 2 DSGVO)
  Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, dann Ausnahmen von Betroffenenrechten, wenn diese sonst die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung des Forschungszweckes notwendig sind.

Markt-, Meinungs- und Sozialforschung

Auch künftig:

- Trennungsgebot
- Pseudonymisierung
- Anonymisierung
- strengere berufsrechtliche Regelungen
- Qualitätsnormen (ISO 20252)

Markt-, Meinungs- und Sozialforschung

Fazit:

Durch die DSGVO keine Lockerung für die Marktforschung, aber auch keine Verschärfung

Die DSGVO bildet eine neue rechtliche Grundlage, Raum für Interpretationen, weniger spezifische nationale Regelungen

EU-Datenschutzgrundverordnung & Marktforschung

Danke.

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e.V.
holger.muehlbauer@teletrust.de