An den Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder

Bericht des Ordensdatenschutzbeauftragten der Congregatio Fratrum Cellitarum seu Alexianorum

für die Zeit vom 01.01.2018 – 31.12.2018

Die Datenschutzaufsicht erstellt gemäß § 44 Abs. 6 KDR-OG jährlich einen Tätigkeitsbericht, der dem Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder vorgelegt und der Öffentlichkeit zugänglich gemacht wird. Dieser Tätigkeitsbericht enthält eine Darstellung der wesentlichen Entwicklungen des Datenschutzes im kirchlichen sowie nichtkirchlichen Bereich.

I. Reform des EU-Datenschutzrechts

Das Berichtsjahr war geprägt von der Reform des EU-Datenschutzrechts aufgrund der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (kurz „Datenschutz-Grundverordnung“ bzw. „DSGVO“ genannt).

1. Zentrale Inhalte

Hintergrund der DSGVO war der Wunsch nach Harmonisierung und Vereinfachung des europäischen Datenschutzes. Zentrale Bereiche mit dem umfangreichsten Anpassungsbedarf sind u. a.:

» Erweiterung der Anforderungen an die IT-Sicherheit mit umfassender Risikobetrachtung/-bewertung (Accountability-Prinzip)
» erweiterte Informations- und Auskunftspflichten zugunsten der Betroffenen
» neue Anforderungen an die Auftragsdatenverarbeitung
» Gemeinsam für die Verarbeitung Verantwortliche als neue Form der Zusammenarbeit mit insbesondere formalen (vertraglichen) Anforderungen
» erweiterte Meldepflichten bei Datenpannen
» erweiterte Rechenschafts- und Dokumentationspflichten
» Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Vorsteinstellungen (data protection by design / data protection by default)
» Formalisierung hinsichtlich der Datenschutz-Folgenabschätzung (bisher Vorabkontrolle)

Neben inhaltlichen Neuregelungen besteht ein Kernpunkt der Datenschutzreform in der Einführung hoher Sanktionen bei Datenschutzverstößen. So sieht die DSGVO ein gänzlich neues Sanktionsmodell vor, das an wettbewerbs-/kartellrechtliche Vorgaben angelehnt ist. Insbesondere der Bußgeldrahmen wird auf Beträge von bis zu 20.000.000 EUR bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres des Unternehmens angehoben; ausschlaggebend ist die jeweils höhere Summe.

2. Missverständnisse im Umfeld der DSGVO

Insbesondere kurz vor dem 25. Mai 2018 und dem damit verbundenen Start der DSGVO kam zunehmend „Bewegung“ in die öffentliche Berichterstattung: Ängste vor Abmahnungen, Aufforderung zur Einwilligung in die Datenverarbeitung, Gerüchte über neue Auskunfts- und Löschrechte durch den Betroffenen, Aufforderung zur Unterzeichnung von Verträgen zur Auftragsverarbeitung. Gerne entkräften wir nachfolgend ein paar „Falschmeldungen“:

» Abmahnungen: Hierbei ist die befürchtete „Welle“ nach unseren Erfahrungen ausgeblieben.

» Aufforderung zur Einwilligung in die Datenverarbeitung: Dies ist in der Regel nicht erforderlich gewesen. Zum einen ist eine rechtsgültige Einwilligung, die vor dem 25.05.2018 erteilt wurde, auch nach diesem Tag gültig. Zum anderen ist auch weiterhin – anders als zum Teil kolportiert – eine Datenverarbeitung möglich, die nicht auf einer Einwilligung basiert, wie beispielsweise auf Basis eines Vertrags oder einer anderen Rechtsgrundlage.

» Auskunfts- und Löschrechte: Auch wenn die Rechte der Betroffenen durch die DSGVO etwas modifiziert wurden, so waren diese Rechte auch in vorherigen Gesetzen enthalten und sind nicht gänzlich neu. Dennoch gilt: Ein Betroffener hat nicht nur das Recht, Auskunft über die über ihn verarbeiteten Daten zu verlangen, sondern auch eine Kopie dieser Daten zu erhalten. Auch sind Daten dann zu löschen, wenn der Zweck für die Datenverarbeitung entfällt (beispielsweise nach Vertragskündigung und den steuerrechtlichen Aufbewahrungspflichten).

» Auftragsverarbeitung: Es schien vielerorts die Auffassung vertreten worden zu sein, dass für jede Datenübermittlung an einen Vertragspartner ein Vertrag zur Auftragsverarbeitung erforderlich ist. Hierbei hat sich (größtenteils auch inhaltlich) gegenüber der vorherigen Rechtsauffassung aber nichts geändert.

3. Auftragsverarbeitung

Die Auftragsverarbeitung ist in Artikel 28 der DSGVO geregelt. Zwischen Auftraggeber und Auftragsverarbeiter muss ein Vertragsverhältnis bestehen. Es kommen immer wieder Fragen auf, wann eine Auftragsverarbeitung vorliegt. Folgende Kriterien sprechen allgemein für eine Auftragsverarbeitung:

» keine eigenen Entscheidungsbefugnisse des Auftragsverarbeiters im Hinblick auf die Datenverarbeitung;

» keine Übertragung von Nutzungsrechten an den personenbezogenen Daten;

» fehlende Beziehung des Auftragsverarbeiters zum Betroffenen;

» keine Abgabe der den bloßen Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecken an den Auftragsverarbeiter;

» Kontrollmöglichkeiten des Auftraggebers.

Als klassische Beispiele für eine Auftragsverarbeitung gelten Wartung und Betrieb von IT-Systemen (Software, Hosting, Cloud-Dienste etc.), Personalabrechnung, Lettershop, externes Rechenzentrum oder Vernichtung von Datenträgern/Unterlagen.

4. EuGH-Urteile zur gemeinsamen Verantwortung

Die DSGVO führte das Konstrukt der gemeinsamen Verantwortung in Artikel 26 DSGVO ein. Im Laufe des Jahrs 2018 erließ der EuGH mehrere Urteile gemeinsame Verantwortliche betreffend, welche die voranschreitende Relevanz verdeutlichen:

a) C-210/16, EuGH *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein gegen Wirtschaftsakademie Schleswig-Holstein GmbH* (Beteiligter u.a.: Facebook Ireland Ltd)

Der EuGH entschied am 05.06.2018, dass der Betreiber einer Facebook Fanpage und Facebook für die Datenverarbeitung gemeinsam verantwortlich sind. In dem Zusammenhang stellte der EuGH klar, dass gemeinsame Verantwortung nicht zwangsläufig gleichwertige Verantwortung bedeutet. Die von Facebook zur Verfügung gestellte Insights-Vereinbarung ist jedoch unzureichend ausgestaltet. Zu bemängeln ist eine hinreichende Konkretisierung der verarbeiteten personenbezogenen Daten. Mithin fehlt es auch an ausreichender Transparenz.

b) C-25/17 EuGH, Verfahren auf Betreiben des Tietosuojavaltuutettu, Beteiligte: Zeugen Jehovas

Der EuGH entschied auf Betreiben des Tietosuojavaltuutettu (Data Protection Ombudsman von Finnland), dass die Gemeinschaft der Zeugen Jehovas und ihre jeweiligen Mitglieder gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO sind. Bereits die Anfertigung handschriftlicher Notizen nach Straßenzügen ist ausreichend strukturiert für eine Datenverarbeitung, da handschriftliche Notizen für die Auffindbarkeit ausreichen.

II. Auswirkungen auf nationales Datenschutzrecht

Im Zuge der DSGVO ergab sich auch eine Novellierung des Bundesdatenschutzgesetzes (BDSG). Das BDSG neu trat zeitgleich mit der DSGVO in Kraft. Die DSGVO gilt in den EU-Mitgliedsstaaten als unmittelbares Recht und geht nationalen Gesetzen vor. Das BDSG kommt im Rahmen von fakultativen und obligatorischen Öffnungsklauseln der DSGVO nach seiner Anpassung weiter zur Anwendung. Die Öffnungsklauseln gaben den nationalen Gesetzgebern Spielraum in bestimmten Bereichen nationale Datenschutzgesetzgebung zu gestalten. Die DSGVO wird also durch das BDSG konkretisiert und ergänzt.

So wurde beispielsweise das Recht von Betroffenen auf Löschung durch § 35 Abs. 3 BDSG eingeschränkt, wenn der Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.

Das BDSG konkretisiert zudem Art. 9 Abs. 2 lit. j DSGVO. Dieser Artikel besagt, dass die Verarbeitung besonderer Kategorien von personenbezogenen Daten wie ethnische Herkunft

oder religiöse Überzeugungen auf der Grundlage des nationalen Rechts eines E-Mitgliedsstaates bspw. für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig sein kann, wenn die Verarbeitung für diese Zwecke erforderlich ist und in einem angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht.

§§ 50, 45 BDSG konkretisieren, dass diese Verarbeitung in archivarischer, wissenschaftlicher und statistischer Form durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten zuständigen öffentlichen Stellen zum Zweck der Erfüllung dieser Aufgaben nur zulässig sei, wenn geeignete Garantien für die Rechtsgüter der Betroffenen geschaffen werden. Beispielhaft genannt sind eine zeitnahe Anonymisierung der personenbezogenen Daten der Betroffenen oder Vorkehrungen gegen die Kenntnisnahme der Daten durch Unbefugte.

III. Auswirkungen auf kirchliches Recht

Die DSGVO achtet den Status, welchen Kirchen, religiösen Vereinigungen oder Gemeinschaften in den EU-Mitgliedstaaten nach den dort geltenden verfassungsrechtlichen Vorschriften genießen. Gemäß Art. 91 DGSVO, ErwG 165 i. V. m. Art. 17 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV). dürfen die genannten Institutionen eigene Regelungen zum Datenschutz treffen. Hierbei sind jedoch die Regelungen der DSGVO zu beachten. Im Zuge der EU-Datenschutzreform trat auch das neue Gesetz über den Kirchlichen Datenschutz (KDG) im Mai 2018 in Kraft. Diese ersetzt die bisherige Anordnung über den kirchlichen Datenschutz (KDO). Das KDG wird von den Diözesen und diesen zugeordneten Einrichtungen angewendet. Für Ordensgemeinschaften päpstlichen Rechts trat am 24.05.2018 die Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) in Kraft. Die Durchführungsverordnung (KDO-DVO) bleibt bis zu einer Neuregelung, jedoch längstens bis zum 30.06.2019, bestehen.

IV. Tätigkeiten

Es wurden im Berichtszeitraum keine Datenschutzverletzungen gemeldet. Zudem machten Betroffene weder von Ihren Betroffenenrechten Gebrauch noch gingen Beschwerden ein.

Schulungen zum Datenschutz wurden angeboten.

Tätigkeit	
Datenpanne	keine
Auskunftsersuchen	keine

Tätigkeit	
Beschwerden	keine
Schulungen	wurden angeboten

Dr. Heiko Haaz

Ordensdatenschutzbeauftragter