An den Höheren Oberen der Ordensgemeinschaft der Alexianerbrüder

Bericht des Ordensdatenschutzbeauftragten der Congregatio Fratrum Cellitarum seu Alexianorum

für die Zeit vom 01.01.2019 – 31.12.2019

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. ePrivacy Verordnung

Zum Zeitpunkt des Inkrafttretens der DSGVO war eigentlich geplant, dass die auch die ePrivacy Verordnung in Kraft tritt. Zum einen wäre dadurch die ePrivacy Richtlinie von 2002 upgedatet worden und zum anderen sollte die ePrivacy Verordnung anders als die DSGVO spezielle Regelungen für den Online-Bereich enthalten (z. B. Tracking auf Webseiten, Online Werbung). Dadurch würden sich DSGVO und ePrivacy Verordnung komplementieren. Die Verhandlungen über die ePrivacy Verordnung zogen sich jedoch hin. Einigen EU-Mitgliedsstaaten ging der Entwurf zu weit. Hingegen andere EU-Mitgliedsstaaten ging der Entwurf nicht weit genug. Unter finnischer Ratspräsidentschaft wurde ein Kompromissvorschlag eingereicht, der Ende 2019 jedoch ebenfalls nicht angenommen wurde. Wann oder ob die Verhandlungen wieder aufgenommen werden ist noch in der Schwebe.

II. Datenschutzanpassungsgesetz

Das Jahr 2019 brachte das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (2. DSAnpUG) mit sich. Betroffen sind von dem Paket insgesamt 154 einzelne Gesetze. Dieses Gesetz diente dazu nationale Gesetze, die Regelungen zum Datenschutz enthalten, an die am 25. Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) anzupassen.

III. Durchführungsverordnung über den kirchlichen Datenschutz

Zudem trat auch die neue Durchführungsverordnung über den kirchlichen Datenschutz (KDG-DVO) in Kraft. Diese enthält Ausführungsbestimmungen zum KDG für die kirchlichen

Stellen, welche der Diözesen sowie den Verband der Diözesen Deutschland zugeordnet sind. Die KDG-DVO löste hiermit die Anordnung über den kirchlichen Datenschutz (KDO) ab.

In einzelnen Diözesen gelten Patientendatenschutzordnungen. Die katholische Kirche ist weiterhin um eine Neuregelung bemüht, welche die bestehenden Patientendatenschutzordnungen harmonisieren und für alle Diözesen und Erzdiözesen gelten soll.

IV. Facebook „Like"-Button

Durch die zunehmende Digitalisierung setzt sich der Trend fort, dass sich die zentralen Themen auf den Einsatz von Software sowie Sozialen Medien beziehen.

In C-40/17 EuGH, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* entschied der Europäische Gerichtshof, dass sowohl Facebook als auch der Betreiber einer Internetseite, in welche „Gefällt mir"-Buttons eingebettet sind gemeinsam verantwortlich sind. Daraus folgt: Die Nutzer müssen über Ausmaß, Art und Zweck der Datenverarbeitung vom Website-Betreiber informiert werden.

Die Fashion ID, ein Onlineangebot der Modekette Peek & Cloppenburg, band auf der Website den als Like-Button bekannten „Gefällt mir"-Button so ein, dass Nutzer direkt auf Facebook bekunden konnten, dass sie ein bestimmtes Produkt mögen. Allerdings wurden bereits beim Besuch der Seite die personenbezogenen Daten des Nutzers an Facebook übermittelt – egal, ob der Button überhaupt angeklickt wurde; sofern es sich um ein Facebook-Mitglied handelt, werden die Daten auch dem Account personenbezogen zugeordnet. Der Like-Button übertrug beim Laden der Seite die IP-Adresse, die Webbrowser-Kennung sowie Datum und Uhrzeit des Aufrufs.

Die Einbindung des Buttons ohne Zustimmung der Nutzer ist datenschutzrechtlich nicht in Ordnung, wenn dadurch personenbezogene Daten an den Anbieter des Plug-ins übermittelt werden. Der Button optimiere die Werbung für die Produkte von Fashion ID und mache diese bei Facebook sichtbarer. Das sei ein wirtschaftlicher Vorteil, so dass Fashion ID „zumindest stillschweigend" der Erhebung personenbezogener Daten von den Website-Besuchern akzeptiert habe. Für die spätere Datenverarbeitung durch Facebook könne der Betreiber allerdings nicht verantwortlich gemacht werden.

Der bekannte Cookie-Hinweis weitet sich nun auch auf den „Gefällt mir"-Button aus. Wenn Unternehmen künftig Einwilligungen von den Nutzern einholen, reicht kein pauschales „okay". Der Website-Betreiber muss präzise und verständlich über die Datenverarbeitung informieren und darlegen, was mit den Daten des Nutzers passiert.

In diesem Zusammenhang verweisen wir auch auf unsere Ausführungen zu Facebook-Fanpages in unserem Bericht vom Vorjahr.

V. EuGH-Urteil zum Einsatz von Cookies

Am 01.10.2019 erging ein Urteil des EuGHs in der Rechtssache C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e. V. gegen Planet49 GmbH*, in welchem die Fragen nach der Rechtsgrundlage zum Einsatz von Cookies sowie die Modalitäten dazu und zu erteilenden Informationen beantwortet wurden.

Es wurde entschieden, dass der Einsatz von nicht notwendigen Cookies einer Einwilligung bedarf. Nun ist immer eine transparente Information der Betroffenen und eine aktive Handlung erforderlich, sodass es nicht mehr ausreichend ist, vorangekreuzte Auswahlen oder reine Bestätigungsbuttons im Cookie-Banner zu implementieren.

VI. Nutzung von WhatsApp

In der Praxis taucht immer wieder die Frage auf, ob man WhatsApp nicht doch nutzen kann. Der Einsatz von WhatsApp ist weiterhin problematisch. WhatsApp liest bei der Installation der App das Telefonbuch des Nutzers aus. Diese Daten werden mit den in der Datenbank von WhatsApp gespeicherten Bestandsdaten abgeglichen. Diese Datenverarbeitung erfolgt unabhängig davon, ob es sich um Telefonnummern von Personen handelt, die WhatsApp ebenfalls nutzen, oder ob es sich um Telefonnummern von Personen handelt, die WhatsApp nicht nutzen. Die Verarbeitung der Daten durch WhatsApp erfolgt zu dem unabhängig davon, ob die Betroffenen mit der Datenverarbeitung einverstanden sind oder nicht sowie unabhängig davon, ob Sie von der Datenverarbeitung Kenntnis haben oder nicht.

VII. Problematischer Einsatz von Office 365

Microsoft Office 365 ist eine Kombination bestehend aus einem Online-Dienst, einer Office-Web-Anwendung und einem Office-Software-Abonnement. Im Herbst letzten Jahres kam die niederländische Regierung in einer Untersuchung zu Office 365 zu dem Ergebnis: Microsoft verstoße gegen die EU-Datenschutz-Grundverordnung (DSGVO). Zentraler Vorwurf: Microsoft sammele systematisch und in großem Umfang Daten über die individuelle Nutzung von Word, Excel, PowerPoint und Outlook. Dies erfolge ohne, dass die Nutzer oder der Anwender (einsetzendes Unternehmen) darüber informiert würden. Microsoft biete keine Wahl in Bezug auf die Datenmenge, die Sammlung auszuschalten, oder die Möglichkeit, zu sehen, welche Daten gesammelt werden, da der Datenstrom verschlüsselt ist.

Die niederländische Regierung traf Verabredungen in Vertragsqualität mit dem US-Softwaregiganten. Microsoft sagte Änderungen zu, die eine DSGVO-Kompatibilität sicherstellen sollten. Was genau verändert werden sollte, teilte der US-Konzern der interessierten Öffentlichkeit allerdings nie genau mit. Es blieb bei vagen Ankündigungen und Verlautbarungen vom Firmensitz in Redmond.

Durch die von Microsoft bislang getroffenen Maßnahmen ist nach unabhängigen Untersuchungen ein relativ hohes Datenschutzniveau für Inhaltsdaten erreicht. Allerdings bestehen weiterhin Risiken, welche durch die Verarbeitung der umfassenden Telemetrie- und Diagnosedaten verursacht werden. Außerdem muss die Frage gestellt werden: Kann ein „normaler Anwender“ dieselben Nebenabreden und Vereinbarungen mit Microsoft treffen, wie es die niederländische Regierung getan hat? Es ergibt sich für die Verantwortlichen die Notwendigkeit einer Datenschutzfolgenabschätzung. Eine Konsultation der Aufsichtsbehörde kann dabei notwendig sein. Denn ungeklärt und hochproblematisch bleibt es, dass nicht alle Risiken vom Anwender selbst entschärft werden können, sondern die Mitwirkung von Microsoft notwendig ist. Zum jetzigen Zeitpunkt kann aufgrund der Faktenlage nicht von der Möglichkeit eines datenschutzkonformen Einsatzes ausgegangen werden.

VIII. Bundesverwaltungsgericht zur Videoüberwachung

Zunehmend ist auch im kirchlichen Bereich Videoüberwachung im Einsatz. Das Bundesverwaltungsgericht (BVerwG) befasste sich jüngst mit einem Fall zur Videoüberwachung. Der Fall ist exemplarisch für private Videoüberwachung und hilft sicherlich bei der Klarstellung ähnlich gelagerter Fälle. Folgender Sachverhalt lag dem BVerwG zur Entscheidung vor: Die Klägerin ist Zahnärztin. Ihre Praxis kann durch Öffnen der Eingangstür ungehindert betreten werden. Der Empfangstresen ist nicht besetzt. Die Zahnärztin brachte oberhalb dieses Tresens eine Videokamera an. Die aufgenommenen Bilder können in Echtzeit auf Monitoren angesehen werden, die die Klägerin in Behandlungszimmern aufgestellt hat (sog. Kamera-Monitor-System). Die Brandenburger Landesdatenschutzbeauftragte gab der Zahnärztin auf, die Videokamera so auszurichten, dass der zugängliche Bereich vor dem Empfangstresen, das Wartezimmer und der Flur zwischen Eingangstür und Tresen nicht mehr erfasst werden. Hiergegen klagte die Zahnärztin.

Auch wenn das Gericht zum Ergebnis kam, dass die DSGVO im konkreten Fall keine Anwendung fand, weil der Vorfall vor dem 25.05.2018 (also dem Beginn der Gültigkeit der DSGVO) geschah, kam das BVerwG in seinem Urteil zum Ergebnis, dass die Zulässigkeit von Videoüberwachungen zu privaten Zwecken sich nunmehr nach Art. 6 Abs. 1 Nr. 1 lit. f DSGVO richtet. Konkret bedeutet dies: Private Videokameras können im Ergebnis nur auf der Rechtsgrundlage des Art. 6 Abs. 1 Nr. 1 lit. f DSGVO (Interessensabwägung) und damit auf Unionsrecht betrieben werden. Die danach zu erfolgende Güterabwägung ist nicht durch nationales Recht modifizierbar, wie es im § 4 BDSG n. F. geschehen ist. Vielmehr ist der BDSG-Regelungstatbestand nicht EU-rechtskonform.

IX. Informationspflicht

Immer wieder werden „Medienbrüche“ bei der Übermittlung der Informationspflicht gemäß Art. 13, 14 thematisiert. Die zentrale Frage ist eigentlich nicht, ob ein Medienbruch vorliegt, sondern ob rechtzeitig und vollständig informiert wird. Die Betroffenen müssen spätestens zum Zeitpunkt der Datenerhebung informiert werden.

Man muss die Informationen so anbieten, dass die Betroffenen diese Informationen annehmen können. Wenn man nicht weiß, ob der Betroffene Internet hat, reicht ein Hinweis auf Papier, wo auf einen Link verwiesen wird, nicht aus. Man kann nicht davon ausgehen, dass jede Person einen Internetzugang hat oder auf andere Weise das Internetangebot wahrnehmen kann.

Wenn man also Personen auf Papier anschreibt, sollte die Information nach Art. 13 und 14 DSGVO ebenfalls auf Papier erfolgen. Wenn man sich sicher ist, dass der Betroffene Internet hat, bspw. weil man vom Betroffenen eine E-Mail-Adresse hat, dann wäre ein Hinweis im postalischen Schreiben auf einen Link im Internet ausreichend.

X. Auskunftsrechte

Betroffene haben gemäß Artikel 15 DSGVO ein Auskunftsrecht gegen den Verantwortlichen. Es kommen immer wieder Fragen auf, wenn Auskunftsersuchen im Detail geprüft werden müssen. Hierzu haben wir ein paar Fragen gesammelt.

» Ist es ausreichend, bei der Auskunft nach Artikel 15 DSGVO die Datenkategorien zu nennen (ohne Nennung der konkreten Daten)?

Der Wortlaut des Artikel 15 Abs. 1 DSGVO ist eindeutig. Darin steht: „Die betroffene Person […] hat […] ein Recht auf Auskunft über diese personenbezogenen Daten und auf […] Informationen“. Daher sind auch die konkreten Daten zu nennen. Ohne Nennung der konkreten Daten würde dem Betroffenen die Basis fehlen, um von seinem Recht auf Berichtigung Gebrauch machen zu können.

» Muss sich der Betroffene auch legitimieren, wenn das Auskunftsersuchen über einen Auskunftsplattformservice maschinell gestellt wird? Muss man solche Auskunftsersuchen beantworten?

Auch wenn die Auskunft maschinell (über einen solchen Service) gefordert wird, darf dieses Auskunftsersuchen nicht ignoriert werden. Man muss dann nach der Legitimierung fragen.

Man braucht jedoch nicht notwendigerweise immer einen Legitimationsnachweis, obschon es Fälle gibt, wo es angebracht ist, einen solchen zu fordern. Wenn die Auskunft per Briefpost gefordert wird, ist es auch in Ordnung, wenn die Auskunft per Post an die im Kundendatensatz hinterlegte Adresse ohne Prüfung der Legitimation erfolgt.

» Ist es zur Befriedigung eines Auskunftsverlangens nach Artikel 15 DSGVO ausreichend bezüglich der Zwecke, der Rechtsgrundlage und der Dauer der Verarbeitungen auf die Informationen nach Artikel 13 und 14 DSGVO zu verweisen?

Es ist mittlerweile geübte Praxis, dass Verantwortliche zur Beauskunftung anstelle einer konkreten Benennung auf die Informationen verweisen. Dies führt dazu, dass der Betroffene die einzelnen Daten/Datenkategorien nicht einer konkreten Verarbeitung zuordnen kann. Dies wiederum führt zu einer Intransparenz in Bezug auf die Verarbeitung personenbezogener Daten. Daher genügt dies nicht, weil in Artikel 13 und 14 DSGVO nicht die konkreten Daten stehen; für gewöhnlich sind nicht einmal in den Informationsblättern alle Datenkategorien genannt.

XI. Tätigkeiten

In 2019 wurden 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
Beschwerden	keine
Schulungen	wurden angeboten

Dr. Heiko Haaz

Ordensdatenschutzbeauftragter