Sehr geehrter Herr Pfarrer,
sehr geehrte Damen und Herren des Verwaltungsrates,
sehr geehrte Damen und Herren,

hier kommt nun eine etwas längere Rund-Mail, die ich auch in Kürze auf meiner Homepage zum Download anbieten werden. Schauen Sie einfach gelegentlich dort nach.

Über was hat der Europäische Gerichtshof (EuGH) mit Urteil vom 16. Juli 2020 entschieden?

Ziff. 5 der Entscheidung lautet:

"Der Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes ist ungültig."

Vereinfacht gesagt, hat der EuGH u.a. die bisherigen sog. „Privacy Shield"-Regelung der EU-Kommission, die die Übermittlung von personenbezogenen Daten in die USA regelten, für unwirksam erklärt.

Was ist jetzt zu tun?

Ich empfehle Ihnen folgende Vorgehensweise:

1. Ermitteln Sie alle Dienstleister aus den USA, die Sie nutzen, und prüfen Sie, ob für die Übermittlung der Daten in die USA zur Gewährleistung des angemessenen Schutzniveaus allein auf eine „Privacy Shield"-Zertifizierung des Dienstleisters gesetzt wurde oder ob die sog. EU-Standardvertragsklauseln vertraglich vereinbart worden sind.

2. Wenn die Basis nur das „Privacy Shield" ist, prüfen Sie, ob Sie auf den Dienstleister verzichten und das Vertragsverhältnis kündigen können. Das EuGH-Urteil bietet hier ggf. die Möglichkeit einer fristlosen Kündigung.

3. Wenn Sie auf den Dienstleister nicht verzichten können, dann schreiben Sie Ihren Ansprechpartner bei dem Dienstleister an, weisen auf das EuGH-Urteil zur Unwirksamkeit des „Privacy Shields" hin und fragen nach, ob kurzfristig der Abschluss der sog. EU-Standardvertragsklauseln möglich ist.

4. Wenn der Dienstleister nicht bereit sein sollte, die EU-Standardvertragsklauseln abzuschließen, sollte der Dienstleister nach Möglichkeit nicht mehr eingesetzt werden.

5. In bestimmten Fällen bleibt dann nur die Möglichkeit, auf in § 41 KDG enthaltene Ausnahmen zurückzugreifen. Die Aufsichtsbehörden werden allerdings eher eine sehr restriktive Anwendung

dieser Norm zulassen. Das wäre aber immer noch besser als keine Lösung.

6. Wichtig: Jetzt von jedem Betroffenen eine Einwilligung (nach § 41 KDG) einholen zu wollen, ist regelmäßig keine gute Lösung und sollte nur dann genutzt werden, wenn es wirklich keine anderen Alternativen gibt.

Was kann denn passieren, wenn man nichts macht?

In § 50 KDG ist, ähnlich wie in der DSGVO, geregelt, dass jede Person, der wegen eines Verstoßes gegen dieses Gesetz ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen die kirchliche Stelle als Verantwortlicher oder Auftragsverarbeiter hat.

Dass ggf. ein Verstoß vorliegt bekommt "jede Person" auch recht leicht heraus, da die Information über die Drittlandübermittlung nach § 15 Abs. 1 lit. f) KDG in der Datenschutzerkärung enthalten sein muss. Außerdem steht jeder betroffenen Person nach § 17 Abs. 2 KDG ein Auskunftsanspruch hierüber zu.

Es ist in Zukunft durchaus damit zu rechnen, dass Anspruchsteller systematisch z.B. Webseiten nach solchen Datenschutzverstößen durchsuchen, um dann z.B. Schadensersatz oder Schmerzensgeld zu beanspruchen..

Daneben können natürlich auch die Datenschutzaufsichtsbehörden mit ihrem Sanktionsrepertoire tätig werden.

Ich kann also nur empfehlen, sich den Fragestellungen zeitnah (wie man so schön sagt) anzunehmen. Diejenigen, die sich aus der neuen Rechtslage einen monetären Vorteil erhoffen, bleiben bestimmt nicht lange untätig.

Was ist der Durchführungsbeschluss zum "Privacy Shield"?

Das EU-US Privacy Shield ist eine informelle Absprache zwischen der Europäischen Kommission und den Vereinigten Staaten von Amerika. Er beruht auf einem System der Selbstzertifizierung, wonach sich amerikanische Organisationen zu einem Katalog von Datenschutzgrundsätzen verpflichten, die vom Handelsministerium der USA herausgegeben wurden. Er erfasst sowohl die für die Datenverarbeitung Verantwortlichen als auch die Auftragsverarbeiter (Beauftragten) mit der Maßgabe, dass sich die Auftragsverarbeiter vertraglich verpflichten, nur auf Weisung des Verantwortlichen in der EU zu handeln und Letzteren dabei zu unterstützen, Privatpersonen die Wahrnehmung ihrer Rechte im Rahmen der Grundsätze zu erleichtern. Die Kommission fasste am 12. Juli 2016 einen Beschluss, wonach „die Garantien für die Übermittlung von Daten auf der Grundlage des neuen EU-US-Datenschutzschilds den Datenschutzstandards in der EU entsprechen“. Dieser Beschluss legitimiert als Angemessenheitsbeschluss im Sinne des Art. 45 DSGVO damit den Austausch personenbezogener Daten zwischen beiden Staatengemeinschaften.

Welche Rolle spielt der Angemessenheitsbeschluss zum Privacy Shield für den kirchlichen Datenschutz?

Nach § 40 Abs. 1 KDG ist eine Übermittlung personenbezogener Daten an oder in ein Drittland oder an eine internationale Organisation (beide außerhalb der Europäischen Union) zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt und dieser Beschluss wichtigen kirchlichen Interessen nicht entgegensteht. Durch die Ungültigerklärung fehlt nun dieser Angemessenheitsbeschluss für Datenübermittlungen in die USA.

Welche Folge hat die Ungültigkeit des Angemessenheitsbeschlusses vom 12. Juli 2016?

Folge des Urteils des EuGH ist, dass z.B. die Inanspruchnahme von US-Dienstleistern nur auf Basis des sog. „Privacy Shield" seit dem 16, Juli 2020 unzulässig ist und ggf. damit rechtswidrig ist. Aus der Rechtswidrigkeit allein können wiederum unmittelbar Bußgeldrisiken resultieren, sodass hier zügig gehandelt werden muss, um diese Datenverarbeitungen/Datenübermittlungen entweder sofort einzustellen oder auf rechtlich andere Füße zu stellen.

Gibt es andere Rechtsgrundlagen für eine Datenübermittlung in die USA?

Ja, aber!

Eine Drittlandübermittlung könnte auf § 40 Abs. 2 KDG gestützt werden. Diese Vorschrift eröffnet zwei Möglichkeiten:

1. in einem rechtsverbindlichen Instrument werden geeignete Garantien für den Schutz personenbezogener Daten vorgesehen oder

2. der Verantwortliche oder der Auftragsverarbeiter kann nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, davon ausgehen, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen.

Realistisch in Betracht kommt hier Variante 1. Als "rechtsverbindliches Instrument" kommt z.B. mit Dienstleistern ein entsprechender Vertrag in Betracht. In der DSGVO-Welt sind dies die sog. Standardvertragsklauseln der EU gem. Art. 46 Abs. 2 lit. c) DSGVO. Das KDG erwähnt diese Klauseln allerdings nicht, sondern spricht pauschal von einem "rechtsverbindlichen Instrument". Da die Standardvertragsklauseln aber genau für den Fall der Drittlandübermittlung geschaffen wurden, spricht m.E. nichts dagegen, sie auch in der KDG-Welt als "rechtsverbindliches Instrument" einzusetzen (ggf. nach sinnvollen Anpassungen).

Aber:

Auch wenn die Standardvertragsklauseln im jetzigen Szenario die zunächst beste Möglichkeit wären, ist es keine Dauerlösung. Denn auch die Verwendung der EU-Standardvertragsklauseln wird im Falle der USA in vielen Fällen dazu führen, dass Aufsichtsbehörden bei einer Prüfung die jeweilige Datenverarbeitung als unzulässig einschätzen und ahnden können, solange nicht die USA bessere Rechtsschutzmöglichkeiten gegen staatliche Überwachung einräumen. Letzteres ist aber in naher Zukunft wohl nicht zu erwarten.

Oder doch?

Art. 46 DSGVO spricht neben "geeigneten Garantien" von der zusätzlich Voraussetzung für eine Drittlandübermittlung, dass den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. In § 40 KDG wird diese Voraussetzung nicht erwähnt. Hier reichen "geeignete Garantien für den Schutz personenbezogener Daten" aus. In der KDG-Welt kann man also durchaus die Auffassung vertreten, dass der Abschluss von Standardvertragsklauseln mit US-amerikanischen Dienstleistern ausreicht, um eine Befugnis zur Datenübermittlung in die USA zu begründen.

Bei Fragen stehe ich wie immer gerne zur Verfügung. Kommen Sie auf mich zu, wenn Sie Unterstützung benötigen.

Empfänger: Kirchengemeinden, Verwaltungsleitungen, Kita-Koordinator*innen

Informatorisch an: Datenschutzkoordinator*innen, institutionelle Stellen des Bistums,
sonstige ausgewählte Einzelempfänger

Mit freundlichen Grüßen

Michael Hilpüsch
Betrieblicher Datenschutzbeauftragter
der Kirchengemeinden des Bistums Limburg

Zentralstelle
Bischöfliches Ordinariat
Roßmarkt 4, 65549 Limburg

Tel. (06431) 295-159
Fax: (06431) 295-219

E-Mail: Datenschutzbeauftragter-Kirchengemeinden@bistumlimburg.de

www.bdsb-kigem.bistumlimburg.de