Wie soll die Datenschutzaufsicht der Katholischen Kirche in Bayern mit dem Urteil des Europäischen Gerichtshofs (Schrems II) vom 16. Juli 2020 umgehen?

Das bezeichnete Urteil bildet einen ganz klaren Einschnitt in den internationalen Verkehr mit personenbezogenen Daten. Es stellt fest, dass das sogenannte „privacy shield“ keine ausreichende Rechtsgrundlage für den Datenverkehr mit den Vereinigten Staaten bildet. Daneben lässt es allerdings offen, ob andere – jeweils von der Datenschutzaufsicht im einzelnen festzustellende – Vorkehrungen ausreichen könnten, um den Datenverkehr doch wieder zulässig zu machen. In diesem Zusammenhang fällt immer der Begriff „Standardvertragsklauseln“; er weckt bei vielen, die auf den Datenverkehr mit den USA angewiesen sind, die Hoffnung auf eine doch zulässige Lösung. Hier wird es aber wahrscheinlich eng werden, weil der EuGH selbst an anderer Stelle (RN. 185) feststellt, dass die gängigen Inhalte der Standardvertragsklauseln wegen des engmaschigen US-Rechts keine Hilfe bieten.

Es ist vor allem der sogenannte „Cloud Act“, der die Schwierigkeiten macht. Nach diesem Gesetz kann die US-Regierung von allen im Ausland tätigen amerikanischen Gesellschaften verlangen, dass von ihnen gespeicherte Daten den amerikanischen Behörden zur Verfügung gestellte werden (https://en.wikipedia.org/wiki/CLOUD_Act). Entsprechendes gilt für ausländische Unternehmen, die in den USA wirtschaftlich tätig sind. Dem von der Herausgabeverpflichtung betroffenen Unternehmen steht nach dem Gesetz im Einzelfall ein Widerspruchsrecht gegen die Anordnung zur Herausgabe von Daten zu, wenn der Eigentümer der Daten kein US-Bürger ist, nicht in den USA lebt und das Unternehmen durch die Herausgabe der Daten gegen Recht in anderen Ländern verstoßen würde. Dies gilt aber leider nur für Länder, die mit den USA ein Abkommen unter dem CLOUD Act abgeschlossen haben. Aktuell hat lediglich Großbritannien ein solches „Executive Agreement“ unterzeichnet, sodass es diese Möglichkeit für alle anderen Bürger weltweit nicht gibt.

Nach dieser Rechtsnorm spielt es für personenbezogene Daten aus der EU keine Rolle,

- wo sie gespeichert sind und
- was das US-Unternehmen mit seinen Kunden über die Verfügungsbefugnis hinsichtlich der Daten vereinbart hat; es kann sich rechtlich nicht wehren.

Ich – der Datenschutzbeauftragte der bayerischen (Erz-) Diözesen – muss mich nun entscheiden, wie ich mit dieser Rechtslage umgehen will. Auch für den Bereich der katholischen Kirche wird unter anderem die Kommunikation mit den Mitgliedern teilweise schon stark auf die Mitarbeit von US-Unternehmen gestützt. Gerade in der aktuellen Lage benötigen wir momentan manche Programme ganz dringend, z.B. Konferenzprogramme. Abgesehen davon sind kirchliche Verantwortliche aktuell dazu angehalten ihre bisherigen technischen Lösungen an den Wegfall des „privacy shields“ anzupassen – dies wird einige Zeit dauern; bildlich gesprochen: Ein fahrender Zug hat auch einen gehörigen Bremsweg. Und schließlich hege ich noch die Hoffnung, dass sich die USA der EU gegenüber für eine Lösung öffnen, die derjenigen gegenüber Großbritannien entspricht, und dass es zu einer vertraglichen Regelung kommt.

Für eine wirklich dauerhafte Lösung ist es noch zu früh. Ich kann derzeit nur reagieren und muss für jede Lösung die Konsequenzen bedenken und natürlich muss ich auch nach der **Art der Daten** unterscheiden:

Art der Daten	**Rechtliche Einordnung des Datenverkehrs**	**Konsequenz für die Aufsichtsbehörden**
IP-Adressen	Sind personenbezogene Daten nur mit den Listen der Provider, also im Ergebnis fast so wie „pseudonymisierte“ Daten.	Derzeit keine Aktion nötig, solange die Providerlisten im Inland bleiben. Etwas anderes gilt, wenn auch der Provider selbst in den USA wirtschaftlich tätig ist.

Lizenzdaten	Sind eindeutig personenbezogene Daten, wenn die Lizenz auf natürliche Person lautet.	Im Rahmen des § 26 KDG sind derzeit wegen der Pandemiefolgen bei bestehenden Anwendungen, z.B. Meeting-Programmen, Änderungen deswegen nicht zwingend nötig, weil dies den Gesamtbetrieb gefährden würde Es wird aber dringend empfohlen, Benutzernamen zu pseudonymisieren und z.B. nur die Personalnummer zu nennen.
E-Mail	Eindeutig schon dann personenbezogene Daten, wenn die Konten der Teilnehmer auf natürliche Person lauten. Entsprechendes gilt bei Übermittlung der Daten von Dritten.	Versendung von E-Mails an private E-Mail-Anschriften ist schon bisher ohnehin nur mit Einverständnis des Empfängers zulässig. Bei Übermittlung von Drittdaten müsste auch der Dritte eingewilligt haben. Nennt der E-Mail-Inhalt personenbezogene Daten, bedarf es immer der Einwilligung dieser Person.
Cloud-Speicher	Schon bisher unzulässig, z.B. MS-ONE, Dropbox, sofern keine wirksame Verschlüsselung vorhanden.	Es gibt bisher keinen vernünftigen Grund zur Aufhebung des Verbotes
Soziale Netzwerke	Unzulässig wegen Weitergabe der Kontaktdaten jedenfalls bei Facebook, Whats App und Instagram.	Im Rahmen des § 26 KDG sind für ein Verbot entsprechende Abschaltfristen nötig, um den Gesamtbetrieb nicht zu gefährden.
Besondere Kategorien von Daten	Übertragung ohnehin unzulässig im Rahmen des § 29 Abs. 11 KDG.	Besonders bei der Gerätefernwartung ist eine Implementierung von Dummy-Datensätzen zumutbar, wenn keine Einzelfallerlaubnis der Datenschutzaufsicht vorliegt.

Das wirkt alles – zugegebenermaßen – abstrakt und kompliziert. Ich weiß das und werde mich bemühen, im Rahmen des mir eingeräumten Beurteilungsspielraum mit Augenmaß und Blick für den Einzelfall zu beraten und zu entscheiden. Meine Entscheidungsrichtlinien gehen momentan dahin,

- bei bereits in Anwendung befindlichen Verfahren jedenfalls bis zur Überwindung der gegenwärtigen Unsicherheiten akuten Pandemiefolgen keine Änderung zu verlangen, die den Betrieb erheblich erschwert und
- bei neuen Anwendungen aber von vorneherein eine Weichenstellung zu verhindern, die später den Dienststellen unnötige Kosten aufbürdet.

Eines werde ich sicher nicht tun: Ich werde mich nicht auf die Entgegennahme des Arguments (fast) aller Anwender beschränken, die Nutzung von Programmen mit US-Bezug sei alternativlos. Das gilt noch nicht einmal für Google, wobei ich zugeben muss, dass hier die Konkurrenz wie z. B. https://www.startpage.com/ noch am dünnsten gesät ist. Office-Programme gibt es zuhauf; sie sind z. T. sogar kostenlos wie *Libre Office*. Konferenzprogramme bilden immer noch eine ordentliche, aber nicht eben unüberwindbare Hürde:
https://www.e-recht24.de/artikel/datenschutz/12122-videokonferenzen-und-datenschutz-vergleichstest-zoom.html
https://blog.hubspot.de/marketing/software-virtuelle-meetings

Jupp Joachimski
Datenschutzbeauftragter der
bayerischen (Erz-) Diözesen