

Datenschutzthemen – Rückschau 2020 und Ausblick auf 2021

Lesedauer: 10 Minuten

Die gute Nachricht ist, dass zahlreiche „Digitalisierungsvorhaben“ den Datenschutz mit einbeziehen, die schlechte ist, dass kein Gestaltungswille erkennbar ist, die DS-GVO zu modernisieren. Ein subjektiver Überblick soll zum Jahresbeginn einen Blick zurück und einen auf die anstehenden Entwicklungen werfen.

Was gibt es rückwirkend zu betrachten?

1. „Lock-in“-Effekt

Die „Investition“ DS-GVO setzt allein auf Daten, u.a. bedingt durch Art. 8 GRCh. Da ist es schwer, rauszukommen, auch wenn es vielerorts „klemmt“ (s. z.B. zur Evaluation *Roßnagel*, MMR 2020, 657 (661)). Das scheint inzwischen nicht mehr tragisch, weil es auch Nachahmer gibt, so jüngst Kalifornien mit einigen Abweichungen und Ergänzungen im Detail im CPRA.

Datenschutz war im ganzen Jahrzehnt ein Riesenthema dank des *EuGH* (Recht auf Vergessen, Joint Control, Safe Harbor, Cookies, 2020: Privacy Shield ungültig) und der Diskussion zur Umsetzung der DS-GVO. Datenschutz wurde allenthalben propagiert, aber 2020 insbesondere coronabedingt wieder abgebaut, etwa durch Einsatz nicht datenschutzkonformer Videokonferenzsysteme (s. *EDSA v. 23.7.2020* und *DSK v. 23.10.2020*). Zudem: „Die Corona-Pandemie stellt die Beachtung des Beschäftigtendatenschutzes infrage. Wer sich dem Wunsch nach unkomplizierten Lösungen entgegenstellt, droht als unliebsamer Bedenkenräger aus dem Entscheidungsprozess ausgeschlossen zu werden.“ (*Wünschelbaum*, NZA 2020, 612).

2. Alte Themen

Manches entwickelt sich unter der Hand, manches bleibt immer gleich.

a) Rechtsgut(verletzungen) und immaterieller Schaden

Die Entscheidungen zum Ersatz immateriellen Schadens bei Datenschutzverstößen machen den (uralten) Unterschied von Regelungsgegenstand (Daten) und Rechtsgut deutlich: Nicht jeder DS-GVO-Verstoß betrifft automatisch auch das Rechtsgut, dessen Verletzung nach deutschem Recht einen Anspruch auf Ersatz immateriellen Schadens auslöst. Es könnte ein Trend sein, dass sich nun die bislang eher abstrakte Drohung, immateriellen Schaden bei DS-GVO-Verstößen leisten zu müssen, konkretisiert (Verletzung des Auskunftsanspruchs aus Art. 15 Abs. 1 DS-GVO: *ArbG Düsseldorf* ZD 2020, 649; zuspätsprechend bei Gesundheitsdaten: *AG Pforzheim* ZD 2021, 50; ähnlich *ArbG Dresden* ZD 2021, 54; zum Überblick s.a. *Paal*, MMR 2020, 14; *LG Karlsruhe* ZD 2019, 511 stellt auf Persönlichkeitsverletzung ab, ebenso *Wybitul*, NJW 2019, 3265). Auch

beim Bußgeld und dessen Zumessung spielt sich die Suche nach dem eigentlichen Rechtsgut ab (wie *LG Bonn v. 11.11.2020 – 29 OWi 1/20 LG* zeigt).

b) Einwilligung

Die angebliche zweite Säule der Zulässigkeit ist ein Misserfolg, nicht nur aktuell im Umfeld der Corona-Maßnahmen (s. z.B. zu den Grenzen *Samardzic/Becker*, *EuZW* 2020, 646). Als Problem des Menschenverständnisses der DS-GVO, der autonome Betroffene, ist das Instrument essenziell, aber die Anforderungen an den Nachweis der Freiwilligkeit („ohne jeden Zweifel“) sind sehr/zu hoch (s. *EuGH v. 11.11.2020 – C 61/19*: Mit einem Vertrag kann nicht nachgewiesen werden, dass der Kunde seine Einwilligung wirksam erteilt hat, wenn das betreffende Kästchen vor der Unterzeichnung von einem Verantwortlichen der Verkäuferseite vorab angekreuzt wurde; erforderlich ist ein aktives Verhalten dieser Person zum Ausdruck ihrer Einwilligung, *EuGH* ZD 2019, 556 m. Anm. *Hanloser*, Rn. 52 und 54 – Planet49).

c) e-PrivacyVO

Die DS-GVO heißt u.a. deshalb so, weil sie von spezielleren Regelungen flankiert werden soll. Dazu gehört die ePrivacy-VO, die seit Jahren kommen soll. Der deutsche Kompromiss ist im *Ministerrat* gescheitert, die Diskussion also weiterhin offen, nur der Fortschrittsbericht ist übrig geblieben.

3. Schub durch Schrems-II-Entscheidung

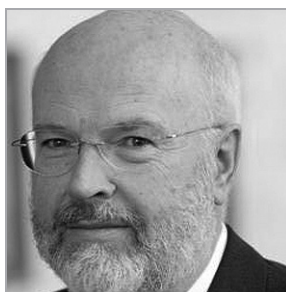
Die Standardvertragsklauseln (SCC) kommen ersatzweise en vogue, nachdem der *EuGH* (ZD 2020, 511 m. Anm. *Moos/Rothkegel* – Schrems II) kurz nach positiver Evaluierung seitens der *Kommission* das Privacy Shield für ungültig erklärte und SCC einen „Freifahrtsschein“ in Leitsatz 4 erteilt hat, wobei in der Begründung ergänzende Regeln nahe gelegt bzw. für erforderlich erachtet werden.

Solche Zusatzvereinbarungen erscheinen mittlerweile gemäß den Bekanntmachungen bzw. Beschlüssen von Aufsichtsgremien, etwa des *EDSA* und der *DSK*, unabweisbar.

Ansichts des Entwurfs neuer SCC v. 12.11.2020 mit neuem System seitens der *Kommission* sind Übergangslösungen bis zur Möglichkeit deren Einbeziehung gefragt. Viele der Defizite, die der *EuGH* für die Ungültigkeit des Privacy Shield anführt, gelten auch für die bisherigen Standardvertragsklauseln, weshalb deren Ergänzung bzw. Erneuerung wichtig ist, sie gelten aber auch für BCRs – sofern Überprüfungs- und eventuell Ergänzungsbedarf besteht.

4. Überwachungsgefahren

Corona-Maßnahmen der Arbeitgeber ließen Videokonferenzsysteme online sprießen, sind aber in Bezug auf den Datenschutz in



Prof. Dr. Jochen Schneider
ist Rechtsanwalt in München und Mitherausgeber der ZD.

Verurf, auch wegen der Kollateral-Erfassung der Familie im Homeoffice, was Gegenmaßnahmen gem. Art. 32 DS-GVO erfordert (vgl. *DSK v. 23.10.2020 – Orientierungshilfe Videokonferenzsysteme*).

Gleichzeitig wächst das Potenzial zur Anwenderüberwachung über die IT auch ohne Homeoffice. So soll laut Medienberichten *Microsoft* die Office-Suite 365 um die Funktionen „Workplace Analytics“ erweitert haben, mit denen die Arbeitsgepflogenheiten der Belegschaft detailliert beobachtet werden können.

5. Auskunft – Kopie

Große Rätsel gibt der Anspruch auf Kopie (Art. 15 Abs. 3 DS-GVO) auf (s. z.B. *LG Heidelberg* ZD 2020, 313 m. Anm. *Zöll/Kielkowski*; *LAG Niedersachsen v. 9.6.2020 – 9 Sa 608/19*; eher restriktiv und ausufernd *LAG Baden-Württemberg* ZD 2019, 276 m. Anm. *Wybitul*). Der Anspruch ist nicht deckungsgleich mit dem Auskunftsanspruch nach Absatz 1 – jedenfalls muss man Absatz 3 angesichts des Wortlauts so interpretieren.

6. Mangel des IT-Produkts bei fehlender Datenschutzkonformität

Immer stärker scheint sich der Ansatz zu verfestigen, dass die DS-GVO zwar nicht direkt die Hersteller adressiere, jedoch fehlende Datenschutzkonformität einen Mangel darstellen könne, evtl. auch ein Haftungsproblem darstelle (*Specht-Riemenschneider*, MMR 2020, 73; *Vásquez/Kroschwald*, MMR 2020, 217; *Potthoff*, ZD 2020, 348). Allmählich dürfte ein Set von Anforderungen zur Erfüllung der Art. 12 ff. und 32 ff. DS-GVO Eingang in die „Requirements“ bei Projekten gefunden haben, wobei aber auch bei käuflich zu erwerbenden Produkten an die nötige Datenschutzzeichnung zu denken ist. Weiteren Auftrieb kann hinsichtlich der Sicherheitseigenschaften die Umsetzung der RL (EU) 2019/770 und 771 bringen (*Spindler/Sinn*, MMR 2019, 488).

Was kommt künftig?

Es kommt ein Jahrzehnt des Datenrechts, innerhalb dessen sich die Defizite der DS-GVO, u.a. die Multi-Relationalität von Daten nicht abbilden zu können, als sehr hinderlich erweisen werden. Es wäre wichtig, die Ebenen der Schutz- bzw. Rechtspositionen und des Umgangs mit Daten stärker zu unterscheiden. Ansätze in der DS-GVO etwa zu „Geheimnis“, „Profilbildung“ oder Transparenzschutz sind schwach. Angeblich ist Big Data anonym möglich, obwohl meist nur Pseudonymisierung erreicht ist oder die Zusatzinformationen für Personenbeziehbarkeit zumindest bei Dritten verfügbar sind (*EuGH* ZD 2017, 24 m. Anm. *Kühling/Klar – Breyer*).

1. DS-GVO-Modernisierung und -Weiterentwicklung

Am Weiterentwicklungsbedarf der DS-GVO besteht kein Zweifel, nicht zuletzt wegen der hohen Änderungsrate bei technischen Entwicklungen und deren Anwendungen. Dass „Digitalisierung“ der falsche Begriff ist, sei nur am Rande erwähnt, eher schlechter noch ist „elektronisch“, wie bei ePA (oder beA).

Besonders interessant ist, dass es der Ethik bedarf, um KI in den Griff zu bekommen (s. *Datenethikkommission*), weil dies die Untauglichkeit der DS-GVO als Regelungsstandard verdeutlicht.

2. Impulse neuer Regelungen?

a) Einwilligung neu konzipieren?

In coronarelevante Verarbeitungen einwilligen – was gilt in Krise und Not als „freiwillig“? Die RL(EU) 2019/770 (DID-RL) birgt eine Kollision zwischen Urheberrecht und Datenschutz (*Sattler*, NJW 2020, 3623 zum Entwurf der Umsetzung): „Es besteht ein grundlegender Konflikt zwischen dem sachlichen Anwendungsbereich der DID-RL (Art. 3 Abs. 1 UAbs. 2 DID-RL) und §§ 327 ff. BGB-RefE und der jederzeitigen Widerruflichkeit der datenschutzrechtlichen Einwilligung (Art. 7 Abs. 3 DS-GVO) einschließlich des sog. Kopplungsverbots (Art. 7 Abs. 4 DS-GVO).“ Damit ist ein wichtiger Hinweis darauf gegeben, die DS-GVO wesentlich stärker für das Vertragsrecht fit zu machen.

b) Das „Einwilligungs-Tabu“

Man darf nicht laut sagen, dass die Einwilligung keine wirkliche Säule des Datenschutzes ist. Wie aber verträgt sich das beharrliche Bestehen auf der Einwilligung, wenn der Betroffene der Verarbeiter ist und die weiteren Konsequenzen aus den einschlägigen Urteilen zu ziehen sind, mit Joint Controllershship für Private und wenn die „Betroffenen“ als primär Verantwortliche zu sehen sind (s.a. zur „privaten“ Datenverarbeitung *Golland*, ZD 2020, 397)? Damit ist aber das Problem der Kollateraldaten bei Instagram, Facebook u.Ä. nicht gelöst.

3. Datenschutzvertragsrecht

Die DS-GVO erzeugt eine Blüte des Datenschutzvertragsrechts. Die Beurteilung der AGB-rechtlichen Wirksamkeit steht erst am Anfang, mit Ausnahme der Beurteilung der Einwilligung. Man kann derzeit davon ausgehen, dass vertragliche Regelungen nicht über Art. 6 lit. b DS-GVO die Zulässigkeit erweitern können. Das verlagert den Schwerpunkt der Auslegung und Ausdehnung noch stärker auf Art. 6 lit. f DS-GVO. Da diese Variante ohnehin schon – trotz des Gebots der Einzelfallprüfung (s. z.B. *Heberlein*, in: *Ehmann/Selmayr*, DS-GVO 2. Aufl. 2018, Art. 6 Rn. 26) – überstrapaziert wird, lässt sich absehen, dass die Gerichte hier Grenzen ziehen werden. Für Auftragsdatenverarbeitung ist der Abschluss des Vertrags konstitutiv (Art. 28 Abs. 3 S. 1 DS-GVO). Ohne Vertrag (oder ein anderes Rechtsinstrument) kommt diese Konstruktion mit gewisser Privilegierungswirkung (deren Umfang strittig ist) nicht zum Zuge. Dafür kommt (ungewollt) Joint Control in Betracht. Die „Gemeinsame Verantwortlichkeit“ bedarf für die Entstehung keiner expliziten vertraglichen Grundlage, nur der Zusammenarbeit. Art. 26 Abs. 1 S. 1 DS-GVO spricht zwar davon, dass die Verantwortlichen in einer Vereinbarung in transparenter Form bestimmte Aspekte festlegen. Das ist aber nicht die Grundlage für das Entstehen des Joint Controllershship.

Die Voraussetzungen des jeweiligen Konstrukts sauber zu differenzieren und Fälle vertraglich klar zu regeln, die Merkmale von Art. 28 und Art. 26 DS-GVO, eventuell in wechselnden Stadien, vereinen, ist sehr schwierig. Der *EuGH* (ZD 2019, 455 m. Anm. *Hanloser – Fashion ID*) legt eine phasenweise Beurteilung nahe. Lässt sich diese auch insoweit anwenden, als die Zusammenarbeit der gleichen Vertragspartner je nach Phase des Bearbeitungsprozesses mal als Auftragsverhältnis, mal als Joint Control gesehen würde, möglicherweise sich überlagernd – also „hybrid“? Letzteres ist deshalb sehr heikel, weil das Merkmal der einseitigen Weisungshoheit des Art. 28 DS-GVO ein gleichzeitiges Nebeneinander kaum zulassen wird. Andererseits deutet sich immer mehr an, dass dann, wenn der Einzelne mit seiner Verwendung der sozialen Medien den „häuslich-familiären“ Sektor verlässt, dieser zum Verantwortlichen – vor allem im Verhältnis zu Dritten – mutiert.

4. Pools and Data Mining

Die Zahl und das Ausmaß der Kooperationen, sowohl innerhalb einzelner Branchen als auch in der Leistungskette, nehmen rasant zu (s. zu Branchenpools *Assion/Hauk*, ZD-Beil. 12/2020). Die Vertragskonstruktionen werden in Kombination mit Cloud-Services bei Wegfall des Privacy Shield noch komplizierter, da ist transparente Gestaltung gefragt: Leistungsvertrag mit zahlreichen Anlagen (u.a. zu SLA), AVV mit Anlage, insbesondere zu TOM, Einwilligungsformulare, Datenschutzerklärung, Regeln zu Auftragnehmern im Nicht-EU-Ausland/SCC und Ergänzungen dazu gemäß etwa Vorgaben der Aufsichtsbehörden und Annexe dazu.

Die Auswertung der ohnehin im Einzugsbereich verarbeiteten Daten zu übergreifenden und weiten Zwecken hat Konjunktur. Hier könnte mit Blick auf die fehlende Transparenz solcher Gestaltung das AGB-Recht zur Bremse werden. Als weitere „Baustelle“ zeigt sich das Kartellrecht (s. z.B. *Podszun*, GRUR 2020, 1268).

5. Sicherheit

Mit Blick auf die Folgen der Schrems-II-Entscheidung (a.a.O.), die Kritik an den Videokonferenz- und Softwaresystemen und die neuen Geschäftsmodelle kann sich 2021 auch als Jahr der IT-Sicherheit entwickeln (s. nur die zahlreichen Ansätze bei *Riehm/Meier*, MMR 2020, 571).