

Umgang mit der gemeinsamen Verantwortlichkeit in der Praxis

Mit dem Urteil in Sachen „Fashion ID“ (Az. C-40/17) hat der EuGH den Anwendungsbereich der gemeinsamen Verantwortlichkeit weiter konkretisiert. Viele Datenverarbeitungen, die bisher als Auftragsverarbeitungen oder alleinige Verantwortung beurteilt wurden, müssen jetzt neu bewertet werden. Handelt es sich dann um gemeinsame Verantwortlichkeit (oder „Joint Controllership“) gem. Art. 26 DS-GVO muss mit den anderen gemeinsam Verantwortlichen eine Vereinbarung getroffen worden, die den gesetzlichen Anforderungen genügt. Fehlt diese Vereinbarung bestehen Sanktionsrisiken. Außerdem schlägt das Fehlen der Vereinbarung auf viele andere Datenschutzpflichten durch, z.B. das Verzeichnis von Verarbeitungstätigkeiten. Mit dieser Mandanteninformation zeigen wir auf, was die gemeinsame Verantwortlichkeit bedeutet. Zudem fassen wir aktuelle Entwicklungen in der Sanktionspraxis der Aufsichtsbehörden für Sie zusammen.

1. Teil: Was bedeutet gemeinsame Verantwortlichkeit?

An einer gemeinsamen Verantwortlichkeit sind mindestens zwei Parteien beteiligt. Diese verarbeiten einzeln, arbeitsteilig oder jeder für sich allein personenbezogene Daten, wofür die beteiligten Parteien jedoch gemeinsam über die Zwecke („Warum?“) und die Mittel („Wie?“) der Verarbeitung entschieden haben. Diese gemeinsame Entscheidung muss nicht ausdrücklich geschehen, sondern kann auch stillschweigend stattfinden, wenn jede Partei mit dem Vorgehen der anderen Partei einverstanden ist.

Die gemeinsame Verantwortlichkeit führt dazu, dass jede Partei für alle gemeinsamen Verarbeitungen so auch nach außen eintreten muss, als würden die Verarbeitungen durch die Partei selbst durchgeführt. Das gilt nach drei Urteilen des EuGH [EuGH, Urt. v. 5.6.2018 – C-210/16 (Facebook Fanpages); Urt. v. 10.7.2018 – C-25/17 (Zeugen Jehovas); Urt. v. 29.7.2019 - C-40/17 (Fashion ID)] sogar dann, wenn einer der Verantwortlichen gar keinen Zugriff auf die vom anderen Verantwortlichen verarbeiteten Daten hat.

Vereinfacht lässt sich eine gemeinsame Verantwortlichkeit nach dem EuGH wie folgt beschreiben:

Wer die Verarbeitung personenbezogener Daten betroffener Personen durch einen anderen Verantwortlichen veranlasst und an den Ergebnissen dieser Verarbeitung partizipiert, ist gemeinsam mit dem Anderen für die Verarbeitung verantwortlich, wenn beide Parteien wechselseitig zumindest stillschweigend in die Verarbeitung des anderen ‚einwilligen‘. Das gilt auch dann, wenn der Veranlassende zu keinem Zeitpunkt Kenntnis von den verarbeiteten Daten hat.

Ist eine gemeinsame Verantwortlichkeit gegeben, müssen die hieran beteiligten Parteien eine Vereinbarung treffen, wer für die gemeinsame Verarbeitung welche Pflichten aus der DS-GVO übernimmt. Für solche Vereinbarungen gibt es anders als bei der Auftragsverarbeitung keine konkreten Vorgaben, sodass diese sehr unterschiedlich ausfallen können.

Was müssen Sie machen?

Bis zur DS-GVO und den Urteilen des EuGH gab es in der Regel nur Auftragsverarbeitung oder alleinige Verantwortlichkeiten, also Übermittlungen zwischen zwei selbständig handelnden Parteien (gelegentlich auch als sog. „Funktionsübertragung“ bezeichnet). Jetzt gilt es zwischen alleiniger Verantwortlichkeit, gemeinsamer Verantwortlichkeit und Auftragsverarbeitung abzugrenzen, die jeweils eigenen Regeln folgen. Dabei können zwischen zwei Parteien gleichzeitig auch Kombinationen bestehen, z.B. in einem komplexen Outsourcing eine Auftragsverarbeitung wegen eines Teils der Daten sowie eine gemeinsame Verantwortlichkeit wegen eines anderen Teils.

Sie müssen deshalb alle Leistungsbeziehungen zu Dritten (einschließlich der mit Ihnen ggf. verbundenen Unternehmen), bei denen personenbezogene Daten verarbeitet werden, auf die richtige Einordnung prüfen. Ist das geschehen ist danach die Rechtmäßigkeit der Verarbeitung (neu) zu bewerten und ggf. der erforderliche Vertrag zur Auftragsverarbeitung abzuschließen oder die Vereinbarung zur gemeinsamen Verantwortlichkeit zu treffen. Lässt sich das nicht umsetzen, weil die anderen Beteiligten nicht mitspielen oder den Sachverhalt anders bewerten ist eine Risikobewertung vorzunehmen. Im „worst case“ muss die Verarbeitung eingestellt werden. Zur Unterstützung dieser Risikobewertung haben wir die nachfolgenden Aspekte für die gemeinsame Verantwortlichkeit zusammengefasst.

Gemeinsame Verantwortlichkeit und Rechtmäßigkeit der Verarbeitung

Jede Datenverarbeitung bedarf einer Erlaubnis, beispielsweise aus Art. 6 DS-GVO oder bei Beschäftigtendaten aus § 26 BDSG. Das gilt auch für die gemeinsame Verantwortlichkeit. Hier muss sich die Erlaubnis insbesondere auch auf die Offenlegung der Daten gegenüber anderen gemeinsam Verantwortlichen beziehen. In der Regel bleibt die Datenverarbeitung dabei auch rechtmäßig, wenn die Vereinbarung zur gemeinsamen Verantwortlichkeit nicht getroffen worden ist; denn die Vereinbarung ordnet die Beziehungen der Beteiligten in der gemeinsamen Verantwortlichkeit untereinander, lässt aber die anderenfalls Pflicht jedes gemeinsam Verantwortlichen zur vollständigen Erfüllung der DS-GVO gegenüber den betroffenen Personen unberührt.

Aber: Wird die Verarbeitung auf eine Interessensabwägung gemäß Art. 6 Abs. 1 Buchst. f DS-GVO gestützt besteht die Gefahr, dass die gesamte Datenverarbeitung ohne die Vereinbarung der gemeinsam Verantwortlichen rechtswidrig wird. Denn ein wesentliches, schutzwürdiges Interessen der betroffenen Personen dürfte es sein, dass die gemeinsam Verantwortlichen über die Vereinbarung ihr Verhältnis zueinander und damit auch die Pflichtenstellung gegenüber den betroffenen Personen geklärt haben, bevor sie mit der gemeinsamen Verarbeitung beginnen. In diesem Fall dürften deshalb die schutzwürdigen Interessen der betroffenen Personen immer das berechnigte Interesse der gemeinsam Verantwortlichen an der Durchführung der Verarbeitung überwiegen. Damit ist bei solchen Verarbeitungen ohne Vereinbarung der gemeinsam Verantwortlichen regelmäßig die gesamte gemeinsame Verarbeitung unzulässig.

Bußgelder nach der DS-GVO

Jede rechtswidrige Datenverarbeitung erfüllt für sich genommen bereits einen Bußgeldtatbestand nach Art. 83 DS-GVO. Dazu kommen weitere Verstöße, die mit einer rechtswidrigen Verarbeitung in gemeinsamer Verantwortlichkeit typischerweise verbunden sein können. Das können u.a. sein:

- Datenverarbeitung ohne Rechtsgrundlage nach Art. 6 DS-GVO; bußgeldbewehrt nach Art. 83 Abs. 5 Buchst. a DS-GVO (bis 20 Mio. Euro bzw. 4% des weltweiten Vorjahresumsatzes)
- Verstoß gegen die Informationspflichten nach Art. 13, 14, 21 DS-GVO; bußgeldbewehrt nach Art. 83 Abs. 5 Buchst. b DS-GVO (bis 20 Mio. Euro bzw. 4% des weltweiten Vorjahresumsatzes)
- Verstoß gegen die Pflicht, den wesentlichen Inhalt des Vertrags über die gemeinsame Verantwortlichkeit den betroffenen Personen zur Verfügung zu stellen nach Art. 26 Abs. 2 Satz 2 DS-GVO; bußgeldbewehrt nach Art. 83 Abs. 4 Buchst. a DS-GVO (bis 10 Mio. Euro bzw. 2% des weltweiten Vorjahresumsatzes)

Wettbewerbsrechtliche Haftung nach dem UWG

Ob Verstöße gegen datenschutzrechtliche Bestimmungen zugleich auch Wettbewerbsverstöße sind und von Wettbewerbern nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) verfolgt und abgemahnt werden können, ist unter Juristen und Gerichten umstritten. Bei der gemeinsamen Verantwortlichkeit besteht das Risiko, nicht nur für solche Datenschutzverletzungen in Anspruch genommen zu werden, die Sie selbst zu verantworten haben, sondern auch für Verstöße der anderen Beteiligten. Umso wichtiger ist es, den Umfang einer gemeinsamen Verantwortlichkeit klar zu erkennen und zu dokumentieren. Beachten Sie: Auch Verbraucherverbände können gegen Datenschutzverletzungen in bestimmten Fällen vorgehen.

Vertragliche Haftung

Für Unternehmen, die schwerpunktmäßig Datenverarbeitungen mit oder für Dritte(n) durchführen oder hierauf gerichtete Leistungen im Markt anbieten, besteht die Gefahr einer zivilrechtlichen Inanspruchnahme durch deren Vertragspartner, wenn diese datenschutzrechtlich wegen Pflichtverletzungen im Zusammenhang mit der gemeinsamen Verantwortlichkeit selbst in Anspruch genommen werden. Zwar sind die Details hier noch ungeklärt, es ist aber denkbar, dass der Anbieter solcher Leistungen vertraglich als Nebenleistung gemäß § 241 Abs. 2 BGB verpflichtet sein kann, seine Kunden auf die gemeinsame Verantwortlichkeit hinzuweisen.

Je stärker sich konkretisiert, wann eine gemeinsame Verantwortlichkeit vorliegt, umso größer wird das Haftungsrisiko für den Anbieter. Er muss dann damit rechnen, dass er von seinen Kunden im Schadensfall auf Freistellung oder Schadensersatz in Anspruch genommen wird, z.B. wenn Kunden Bußgelder (siehe oben) oder eigene Mehraufwände für Dienstleister und

Berater an den Anbieter durchreichen wollen. Deshalb sollte zukünftig das Thema gemeinsame Verantwortlichkeit in Verträgen oder Leistungsbeschreibungen zumindest angesprochen und die Lösung des Anbieters erläutert werden.

2. Teil: Entwicklungen in der aufsichtsbehördlichen Sanktionspraxis

Bei den Aufsichtsbehörden im Datenschutz haben sich zuletzt zwei Entwicklungen ergeben, auf die wir Sie hinweisen. Dies betrifft die Prüfung von Websites, insbesondere wegen der Nutzung von Cookies, durch die Aufsichtsbehörden. Außerdem geht es um die Höhe der in Zukunft zu erwartenden Bußgelder.

Automatisierte Prüfung von Websites

Der Europäische Datenschutzbeauftragte hat kürzlich seine „EDPS Inspection Software“ fertiggestellt und als Open Source zur Verfügung gestellt (Details: https://edps.europa.eu/press-publications/edps-inspection-software_en). Hiermit können Websites automatisiert auf Einhaltung des Datenschutzes geprüft werden. Auch das Bayerische Landesamt für Datenschutzaufsicht arbeitet an einer Anwendung zur automatisierten Prüfung der auf Websites eingesetzten Cookies.

Die Kontrolldichte für Websites dürfte sich damit in Zukunft sprunghaft erhöhen, zumal dort Fehler schnell offensichtlich werden, etwa bei unvollständigen oder falschen Angaben in der Datenschutzerklärung zu den auf der Website eingesetzten Tools und Plugins (siehe unsere Mandanteninformation zu Plugins und Tools aus Juli 2019: <https://kremer-rechtsanwaelte.de/2019/07/30/eugh-entscheidet-fashion-id-einwilligung-fuer-social-plugins-und-tracking-erforderlich/>).

Auf die Datenschutzkonformität der eigenen Website sollte deshalb fortlaufend penibel geachtet werden.

Drastische Erhöhung der Bußgelder

In Deutschland fielen die bekanntgewordenen Bußgelder im Bereich des Datenschutzes bislang sehr niedrig aus, insbesondere im europäischen Vergleich. Die Aufsichtsbehörden haben sich jedoch inzwischen in der Datenschutzkonferenz auf ein gemeinsames Modell zur Berechnung von Bußgeldern verständigt. Ausgehend von den bereits bekannten Informationen handelt es sich um ein sehr komplexes System. Von den bisher bekannten Berechnungsgrundlagen sind zwei besonders bedeutsam:

- Es erfolgt eine starke Orientierung an dem Umsatz des Verantwortlichen (ab 500 Mio. Euro weltweitem Vorjahresumsatz der konkrete Umsatz, andernfalls durch Einteilung in „Umsatzklassen“).
- Aus diesem Umsatz bzw. der Umsatzklasse wird als Bezugsgröße ein Tagessatz (1/360 des Umsatzes) gebildet, aus dem der Bußgeldrahmen (das 1-fache bis 14,4-fache des Tagessatzes) errechnet wird.

Innerhalb dieses Bußgeldrahmens sind weitere Anpassungen möglich, also Senkungen oder Erhöhungen sowie prozentuale Zuschläge für bestimmte Umstände wie eine vorsätzliche Begehung. Das Vorgehen zur Bemessung der Bußgelder nach der oben skizzierten Methode wird bereits angewandt und führt schnell zu sechsstelligen oder höheren Bußgeldern. Der richtige Umgang mit Datenschutzverletzungen wird daher noch einmal wichtiger, sodass entsprechende Prozesse im Unternehmen verankert sein sollten.

Wer sind KREMER RECHTSANWÄLTE?

KREMER RECHTSANWÄLTE ist eine auf Digitalisierungsberatung spezialisierte Sozietät und berät mit insgesamt vierzehn Rechtsanwältinnen und Rechtsanwälten ihre Mandanten und Auftraggeber, darunter DAX-Konzerne, KMU, Kreditinstitute und Finanzdienstleister jeglicher Größe, kirchliche Einrichtungen und Startups, hochspezialisiert an der Schnittstelle zwischen Technik und Recht.

Die Sozietät hat in verschiedenen Branchen- und Dachverbänden an der Umsetzung der DS-GVO durch die jeweiligen Mitglieder mitgewirkt und selbst mehrere Großprojekte zur Umsetzung der DS-GVO erfolgreich geführt oder begleitet. Die Rechtsanwältinnen und Rechtsanwälte veröffentlichen regelmäßig Fachbeiträge, Muster und Bücher zum Datenschutz und sind in der Aus- und Weiterbildung von Datenschutzbeauftragten, Personalverantwortlichen, Juristinnen und Juristen sowie Referendaren und Studierenden tätig.

KREMER RECHTSANWÄLTE ist von der WirtschaftsWoche 2019 als TOP Kanzlei im Datenschutzrecht ausgezeichnet worden. Außerdem wird die Sozietät im kanzleimonitor.de 2018/2019 als von Unternehmensjuristinnen und -juristen empfohlene Kanzlei im IT- und Datenschutzrecht geführt.

Wenn Sie von uns im Datenschutz bereits beraten werden wenden Sie sich bitte an die/den Sie betreuende Rechtsanwältin/Rechtsanwalt. Nehmen Sie anderenfalls jederzeit gerne Kontakt zu einer/einem der folgenden Ansprechpartner/innen auf:

Sascha Kremer, Fachanwalt für IT-Recht, externer Datenschutzbeauftragter (TÜV), sascha.kremer@kremer-recht.de

Daniela Köhnlechner, Rechtsanwältin, Datenschutzbeauftragte (TÜV), daniela.koehnlechner@kremer-recht.de

Per Stöcker, Rechtsanwalt, Datenschutzbeauftragter (ECPC/Maastricht University und TÜV), per.stoecker@kremer-recht.de

Nadine Schneider, Rechtsanwältin, Datenschutzbeauftragte (TÜV), nadine.schneider@kremer-recht.de

Malte Dümeland, Rechtsanwalt, Datenschutzbeauftragter (TÜV), malte.duemeland@kremer-recht.de

Kristof Kamm, Rechtsanwalt, Datenschutzbeauftragter (TÜV), kristof.kamm@kremer-recht.de

Marc Meerkamp, Rechtsanwalt, Datenschutzbeauftragter (TÜV), marc.meerkamp@kremer-recht.de

Alle Ansprechpartner erreichen Sie unter 0221/27141874 und persönlich in der Brückenstraße 21, 50667 Köln (Innenstadt).