



LOSCHELDER

**Newsletter Datenschutzrecht
Dezember 2020**

Sehr geehrte Damen und Herren,

ein ereignisreiches Jahr neigt sich dem Ende zu und verspricht, notgedrungen, besonders ruhig auszuklingen. Auch im Datenschutzrecht haben wir uns nach turbulenten Monaten in unserer letzten Ausgabe 2020 für ruhigere Töne entschieden und weisen Sie auf einen Dauerbrenner hin – datenschutzkonforme Videokonferenzsysteme – sowie zwei interessante Gerichtsentscheidungen. Zuletzt stellen wir, wie immer, interessante Bußgeldfälle aus der EU zusammen.

Wir möchten den Jahresabschluss aber auch dazu nutzen, um Ihnen für ein spannendes Jahr, die vertrauensvolle Zusammenarbeit und den konstruktiven Austausch zu danken. Es war uns – einmal mehr – eine große Freude! Wir wünschen Ihnen und Ihrer Familie frohe Weihnachten und einen guten Start in das neue Jahr 2021.

Wir werden im kommenden Jahr jedenfalls wieder für Sie die datenschutzrechtlichen Entwicklungen aufbereiten und auch in verschiedenen Webinaren persönlich darstellen. Im Februar starten wir eine Digitalisierungsreihe mit drei Terminen – vielleicht finden auch Sie hierbei ein für Sie interessantes Thema, wir würden uns freuen!

Unser Team geht 2021 jedenfalls gestärkt ins Rennen: Wir freuen uns sehr, dass Herr Dr. Simon Kohm zum 01.01.2021 Partner unserer Sozietät wird!

Inhalt

Videokonferenzsysteme

Prüfungspflicht der Aufsichtsbehörde

Schadensersatzpflicht des Datenschutzbeauftragten?

Zu guter Letzt

Videokonferenzsysteme

Videotelefonie gehört zum mittlerweile zum geschäftlichen Alltag, abgewickelt über die verschiedensten Tools. In der datenschutzrechtlichen Kritik stehen sie fast alle. Um dennoch die technischen und organisatorischen Anforderungen bestmöglich zu vereinheitlichen und Standards zu entwickeln, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) nunmehr eine einheitliche [Orientierungshilfe "Videokonferenzsysteme"](#) für Unternehmen, Behörden und andere Organisationen veröffentlicht. In einer daran angelehnten [Checkliste](#) wurden zudem die rechtlichen und technischen Anforderungen an Videokonferenzsysteme in übersichtlicher Form zusammengefasst. Bringt dies nun Klarheit?

Die eindeutige Antwort ist: „Ein wenig“. In technisch-organisatorischer Sicht verlangen die Aufsichtsbehörden folgende Schutzmaßnahmen – fernab von der Einordnung einzelner Anbieter:

- **Videokonferenzen aus dem Home-Office:** Verantwortliche – dies ist in Home-Office-Situationen regelmäßig der Arbeitgeber – haben mittels technischer und organisatorischer Maßnahmen (Art. 25 Abs. 1 DSGVO) sicherzustellen, dass Einblicke in die Privatsphäre der Betroffenen nicht möglich sind (z.B. durch Ausrichtung der Kamera oder durch Einblendung eines virtuellen Hintergrunds). Alternativ kann in solche Einblicke in die Privatsphäre eingewilligt werden (Art. 26 Abs. 2 DSGVO). In jedem Fall muss aber darauf geachtet werden, dass der Betroffene durch den Verantwortlichen über die datenschutzrechtlichen Risiken aufgeklärt wird, die sich aus einer Videokonferenz in den privaten Räumen ergeben.
- **Aufzeichnung der Videokonferenz:** Hierfür muss in der Regel ein eigenständiger Erlaubnisgrund vorliegen. Kommt kein besonderes Dokumentationserfordernis in Betracht, ist grundsätzlich eine Einwilligung aller Teilnehmer in die Aufzeichnung erforderlich. Anderes kann im Einzelfall für offene Veranstaltungen, Publikumsseminare oder öffentliche Vorträge gelten, bei denen eine Aufzeichnung des Vortragenden im Einzelfall erforderlich sein kann. Über die Möglichkeit der Aufzeichnung ist der Betroffene jedenfalls

aber vorab zu informieren, sodass ihm eine echte Möglichkeit bleibt, dieser zuzustimmen, oder sie abzulehnen.

- **Zweckbestimmung und Datensparsamkeit:** Die Datenverarbeitung darf grundsätzlich nur zu dem Zweck der Videokonferenz erfolgen. Weitergehende Verarbeitungen und Auswertungen der Konferenzdaten sind dagegen regelmäßig nicht zulässig. Um so wenige Daten wie möglich zu verarbeiten, sieht die Orientierungshilfe vor, die Teilnehmer der Konferenz in unterschiedliche Rollen einzuteilen, denen entsprechend unterschiedliche Kompetenzen der Verarbeitung zustehen. Hier wird unterschieden zwischen administrativen, moderierenden, präsentierenden und teilnehmenden Personen.
- **Verschlüsselung:** Insbesondere, wenn die Verarbeitung von Daten im Rahmen einer Videokonferenz zu einem hohen Risiko für betroffene Personen führen kann (vor allem wegen der Sensibilität der Daten), müssen der Verantwortliche und gegebenenfalls der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um die Vertraulichkeit der übermittelten Inhaltsdaten auf allen beteiligten IT-Komponenten sicherzustellen. Dies kann beispielsweise über eine Ende-zu-Ende-Verschlüsselung und eine Verschlüsselung gespeicherter Daten erfolgen. Für eine wirksame Ende-zu-Ende-Verschlüsselung ist erforderlich, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentisieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist.
- **Authentifizierung:** Die Voraussetzungen für die Teilnahme an der Videokonferenz sind an das Risiko und die Art der dabei verarbeiteten Daten anzupassen. Bei einem normalen Risiko reicht die Angabe eines Benutzernamens und eines Passworts in der Regel aus. Bei einem hohen Risiko ist eine 2-Faktor-Authentifizierung nach dem Stand der Technik erforderlich.
- **Gastteilnehmer:** Für die Fälle, in denen es für den Einzelfall erforderlich ist, die Risiken einer nicht autorisierten

Teilnahme geringfügig sind und gewährleistet ist, dass nur Personen teilnehmen können, die untereinander bekannt sind und nicht autorisierte Personen erkannt und aktiv ausgeschlossen werden können, ist die Möglichkeit eines Gastzugangs (beispielsweise durch Versenden eines entsprechenden Links) datenschutzrechtlich auch ohne zusätzliche Sicherungsmaßnahmen unbedenklich.

- **Lediglich empfangende Teilnahme:** Teilnehmende müssen die technische Möglichkeit haben, zumindest zeitweise an Konferenzen lediglich empfangend, aber nicht sendend teilzunehmen, d. h. Kamera und Mikrofon auszuschalten. Dabei sind getrennte Deaktivierungsmöglichkeiten für Audio- und Videoübertragung vorzusehen.



Prüfungspflicht der Aufsichtsbehörde

Das Oberverwaltungsgericht Koblenz hatte in einer aktuellen Entscheidung die Gelegenheit, sich zu den Pflichten der Aufsichtsbehörde im Anschluss an eine eingegangene datenschutzrechtliche Beschwerde zu äußern. Wir haben für Sie die wichtigsten Aussagen dieser Entscheidung zusammengestellt.

Der Entscheidung des OVG Koblenz vom 26.10.2020 (Az. 10 A 10613/20) lag die Klage eines Bürgers gegen den LfDI Rheinland-Pfalz zugrunde. Der Kläger war nicht mit den behördlichen Maßnahmen einverstanden, die auf die von ihm

eingereichte Beschwerde folgten. Das OVG kam zu dem Schluss, dass die Behörde durch eine Beschwerde in dreierlei Weisen verpflichtet sei:

- Sie muss sich (1.) überhaupt mit der Beschwerde befassen.
- Sie muss (2.) den angezeigten Beschwerdegegenstand untersuchen.
- Sie muss (3.) den Beschwerdegegner über das Ergebnis der Untersuchung informieren.

Aus dem Umstand, dass eine Beschwerde eingereicht wurde, ergibt sich allerdings kein Recht auf ein konkretes Vorgehen der Behörde oder den Inhalt eines etwaig zu erlassenden Bescheides. Vielmehr steht es der Behörde hier frei, nach pflichtgemäßem Ermessen zu entscheiden.

Für den Fall, dass der Beschwerdeführer mit dem Vorgehen der Behörde nicht einverstanden sei, stehen ihm folgende Alternativen zur Wahl:

- Zum einen kann eine verwaltungsgerichtliche Überprüfung des behördlichen Handelns angestrebt werden. Dabei wird das Gericht wegen des behördlichen Ermessens aber nur eine eingeschränkte Beurteilung vornehmen. Das Gericht wird hier nur feststellen, ob die behördliche Entscheidung ermessensfehlerhaft war, also möglicherweise willkürlich oder sachfremd. Das Gericht wird die Behörde aber in der Regel nicht zu einer konkreten Handlung verpflichten.
- Zum anderen kann der Beschwerdeführer – ganz unabhängig von der Aufsichtsbehörde – gegen den Verantwortlichen der fraglichen Handlung selbst vorgehen. Eine solche Möglichkeit sieht Art. 79 DSGVO ausdrücklich vor, er kann also etwa Schadensersatzansprüche geltend machen.

Das OVG Koblenz recurriert damit in erfreulicher Klarheit auf verwaltungsrechtliche Grundsätze, die generell in Verwaltungsverfahren gelten: Auch die datenschutzrechtlichen Aufsichtsbehörden haben Recht und Gesetz anzuwenden. Eine inhaltlich bestimmte Entscheidung kann ein Beschwerdeführer dagegen regelmäßig nicht beanspruchen. Wenn er mit dem Bescheid einer Aufsichtsbehörde nicht einverstanden ist, kann er gegen diesen vorgehen – oder eben direkt gegen den

Verantwortlichen, dann aber mit deutlich höheren Nachweispflichten.



Schadensersatzpflicht des Datenschutzbeauftragten?

Muss ein Datenschutzbeauftragter den Betroffenen bei rechtswidriger Datenverarbeitung Schadensersatz zahlen? Das LG Landshut hat sich kürzlich mit dieser für alle Datenschutzbeauftragten höchst praxisrelevanten Frage beschäftigt. Wir fassen die wichtigsten Punkte zusammen.

Das LG Landshut lehnte eine Schadensersatzpflicht des Datenschutzbeauftragten über Art. 82 DSGVO gegenüber Betroffenen grundsätzlich ab (Urteil vom 06.11.2020, Az. 51 O 513/20).

Die Begründung aber bleibt interessant: Nach dem überzeugenden Verständnis des Gerichts gilt die gesetzliche Schadensersatzpflicht aus Art. 82 Abs. 1 DSGVO nur für den Verantwortlichen der Datenverarbeitung oder einen Auftragsverarbeiter. „Verantwortlicher“ ist nach Art. 4 Nr. 7 DSGVO jeder, der allein oder gemeinsam mit einem anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Auftragsverarbeiter, wer die Datenverarbeitung im Auftrag des Verantwortlichen durchführt (Art. 4 Nr. 8 DSGVO).

Übt der Datenschutzbeauftragte seine Aufgaben im Einklang insbesondere mit Art. 39 DSGVO aus, wird er niemals derart über Zwecke und Mittel *entscheiden*, auch nicht im Auftrag. Er berät, informiert und überwacht die Entscheidungsträger und ihre Auftragsverarbeiter lediglich über die datenschutzrechtlichen Anforderungen – die Entscheidung (und damit die Schadensersatzpflichtigkeit) aber bleibt stets beim Verantwortlichen selbst, mithin regelmäßig der juristischen Person, in deren Namen die Datenverarbeitung erfolgt.

Davon strikt zu trennen ist die Möglichkeit einer Haftung des Datenschutzbeauftragten etwa im Fall der Falschberatung – derartige Ansprüche stehen dann aber dem Verantwortlichen bzw. Auftragsverarbeiter zu, für den der Datenschutzbeauftragte bestellt ist, nicht den einzelnen Betroffenen.



Zu guter Letzt

Die letzten Wochen waren in Sachen „Bußgelder“ insbesondere in den Nachbarländern spannend. Wir haben Ihnen einige berichtenswerte Fälle aus dem (noch) EU-Umfeld zusammengestellt.

- **Großbritannien: Unzureichende Schutzmaßnahmen**

In Großbritannien verhängte die Datenschutzbehörde gegen den Online-Tickethändler Ticketmaster ein [Bußgeld](#) in Höhe von 1,4 Millionen Euro. Ticketmaster war im Jahr 2018 von mehreren Banken auf Vorkommnisse hingewiesen worden,

die den Verdacht des Betruges zulasten von Ticketmaster-Kunden begründeten. Dennoch unterließ es das Unternehmen nach Behördenfeststellungen, seine Sicherheitsmaßnahmen zu überprüfen. Eine solche Überprüfung war indes gerade deshalb geboten, weil Ticketmaster auf seiner Seite auch Drittdienste implementierte, die besonders anfällig und so besonders kontrollbedürftig waren. Tatsächlich gab es ein Datenleck bei Ticketmaster, von dem rund 9,4 Millionen Nutzer europaweit betroffen waren. Die Datenschutzbehörde erkannte in dem Unterlassen der erforderlichen routinemäßigen – und besonders im Zusammenhang mit den Meldungen notwendigen – Kontrollen einen Verstoß gegen Art. 5 Abs. 1 lit. f, Art. 32 DSGVO.

- **Italien: Fehlende Werbeeinwilligungen**

In Italien wurde gegen ein Telekommunikationsunternehmen ein [Bußgeld](#) in Höhe von 12,25 Millionen Euro verhängt. Grund dafür war, dass das Unternehmen nach Ansicht der Behörde gleich in mehrfacher Weise gegen die Vorgaben aus der DSGVO verstieß: Verarbeitungen ohne Einwilligung lagen in zwei unterschiedlichen Arten vor. Zum einen habe das Unternehmen die Telefonnummern seiner Kunden ohne deren notwendige Einwilligung zu Werbezwecken verwendet. Zum anderen habe das Unternehmen Kontaktlisten von externen Anbietern gekauft und verwendet, ohne dass die betroffenen Personen in die Weitergabe und anschließende Verarbeitung ihrer personenbezogenen Daten einwilligten und ohne, dass eine andere Erlaubnisgrundlage griffe.

Daneben verstieß das Unternehmen nach Ansicht der Behörde auch gegen die Rechenschaftspflicht und trug der Vorgabe des „Privacy by Design“ nicht in ausreichendem Umfang Rechnung. Zuletzt, und von der Datenschutzbehörde besonders hervorgehoben, steht der Umstand, dass sich das Unternehmen auch dem Dienst von Dritt-Callcentern bediente, die für diese Handlungen nicht ausreichend autorisiert gewesen seien. Neben der Zahlung des Bußgeldes wurde das Unternehmen dazu angehalten, Systeme zu implementieren, die sicherstellen, dass personenbezogene Daten nur im Rahmen der erteilten Einwilligung verarbeitet

werden und Betroffene ausführliche Auskunft über die Verarbeitung ihrer Daten erhalten.

- **Norwegen: Rechtswidrige Bonitätsprüfung**

Außerdem verhängte die norwegische Aufsichtsbehörde ein [Bußgeld](#) in Höhe von rund 13.000 Euro gegen ein Unternehmen, weil es ohne die aus Behördensicht notwendige Einwilligung die Bonität eines Einzelunternehmers prüfen ließ, obwohl zu diesem keinerlei unternehmerischen Beziehungen und folglich kein Erlaubnisgrund für die Datenverarbeitung bestanden. Bei der Berechnung des Bußgeldes wurden die Folgen der Corona-Pandemie mildernd berücksichtigt.

- **Spanien: Fehlender Datenschutzbeauftragter**

In Spanien wurde gegen ein privates Sicherheitsunternehmen ein [Bußgeld](#) in Höhe von 50.000 Euro erhoben. Das Unternehmen betrieb ein Videoüberwachungssystem, das alle Personen aufzeichnete, die das Unternehmensgrundstück betraten. Allerdings verfügte das Unternehmen nicht über einen Datenschutzbeauftragten. Den Betroffenen war es so nach Behördenansicht nicht möglich, ihre Rechte aus der DSGVO effektiv umzusetzen. Die Behörde erkannte in dem Fehlen des Datenschutzbeauftragten neben Verstößen nationalen Datenschutzrechts auch einen Verstoß gegen Art. 37 Abs. 1 DSGVO.

- **Spanien: Mangelhafte Zusammenarbeit mit der Aufsichtsbehörde**

In einem anderen Fall verhängte die Datenschutzbehörde ein [Bußgeld](#) in Höhe von 20.000 Euro gegen ein Telekommunikationsunternehmen. Das Unternehmen zeigte sich im Rahmen einer Untersuchung im Zusammenhang mit einem möglichen Datenschutzverstoß wenig kooperativ. So legte es der Behörde im Laufe der Untersuchung unterschiedliche Dokumente vor, sodass die Behörde nicht ausreichend beurteilen konnte, ob ein Verstoß vorgelegen hatte oder nicht. In dem widersprüchlichen und verwirrenden Verhalten sah die Datenschutzbehörde einen eigenen Verstoß gegen Art. 31 i.V.m. Art. 58 Abs. 1 DSGVO.

**Für alle weiteren Fragen rund um das Datenschutzrecht
stehen Ihnen gerne zur Verfügung**



Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de



Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de



Claudia Willmer
+49(0)221 65065-337
claudia.willmer@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE

Partnerschaftsgesellschaft mbB

Konrad-Adenauer-Ufer 11

50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110

info@loschelder.de

www.loschelder.de