

Mögliche Schadenersatzforderungen bei Datenschutzverstößen / Erinnerung an die Löschung von Corona-Daten

Sehr geehrte Datenschutz-Kunden,

in meinem heutigen Datenschutz-Newsletter geht es um zwei unterschiedliche Themen, die nichts miteinander zu tun haben, außer vielleicht, dass aus beiden Sachverhalten eventuell negative Auswirkungen für Verantwortliche erwachsen können:

1. Die Gefahr, an Betroffene für erlittene Datenschutz-Verstöße Schadenersatz bezahlen zu müssen
2. Erinnerung an die Löschung aller personenbezogenen Daten, die in Erfüllung von (gesetzlichen) Vorgaben zur Pandemiebekämpfung verarbeitet wurden.

Datenschutzverstöße sind mit hohen Bußgeldern bewährt

Wer eine Verarbeitung personenbezogener Daten vornimmt bzw. vornehmen muss, also "Verantwortlicher" im Sinne des Art. 4 Abs. 7 EU-DSGVO ist, blickt oft sorgenvoll auf die Bußgelder, die in Art. 83 EU-DSGVO im Falle von Datenschutz-Verstößen aufgerufen werden können. Zur Erinnerung: Bei Verstößen gegen die datenschutzrechtlichen Verpflichtungen eines Verantwortlichen oder eines Auftragsverarbeiters drohen Geldbußen von bis zu 10 Mio. Euro oder bis zu 2 % des erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist. Bei Verstößen gegen die Grundsätze der Verarbeitung, gegen die Wahrung der Betroffenenrechte oder bei der unbefugten Übermittlung personenbezogener Daten in ein Drittland können sich die genannten Werte auch verdoppeln¹⁾. Hinsichtlich der Höhe der im Einzelfall zu verhängenden Bußgelder muss zwar die Verhältnismäßigkeit gewahrt werden, daneben müssen diese aber auch "wirksam" und "abschreckend" sein. Die Auslegung der Aufsichtsbehörden überrascht häufig den wenig mit der Materie befassten Verantwortlichen, zumeist in der Richtung, dass er die verhängten Bußgelder vielfach als unverhältnismäßig hoch bewertet.

Darüber hinaus auch zivilrechtliche Forderungen möglich

Aber kann an einen Verantwortlichen auch zivilrechtlich eine Forderung aus einem Verstoß gegen die EU-DSGVO erwachsen? Eindeutig "Ja", wie das folgende Urteil des Arbeitsgerichts Neuruppin aufzeigt. Im zu verhandelnden Fall hatte eine ehemalige Mitarbeiterin festgestellt, dass sie auf der

Website des Arbeitgebers noch immer als Mitarbeiterin aufgeführt war. Als Tätigkeit war zudem benannt, dass sie als Biologin Wasseranalyseprotokolle schreiben und Kunden betreuen würde. Diese Angaben waren falsch, da die betroffene Mitarbeiterin auch während des Anstellungsverhältnisses nicht in ihrem eigentlichen Beruf, sondern im Bereich des Büromanagements tätig war. Der Verantwortliche hat trotz Aufforderung der Betroffenen die Angaben auf der Website nicht korrigiert bzw. nach ihrem Ausscheiden nicht gelöscht. Die Betroffene klagte daher auf 8.000 EUR Schadenersatz und Abgabe einer Unterlassungserklärung. Die Unterlassungserklärung wurde vom Verantwortlichen abgegeben, er wollte der Klägerin jedoch nur 150 EUR Schadenersatz zugestehen, die er auch bezahlt hat.

In seinem Urteil vom 2021-12-14 (Az. 2 Ca 554/21) hat das Arbeitsgericht der Klägerin 1.000 EUR Schadenersatz zugebilligt, die bereits bezahlten 150 EUR wurden auf die festgesetzte Schadenssumme angerechnet. Das Urteil zeigt zum einen, dass Datenschutzverstöße zu direkten Forderungen betroffener Personen an Verantwortliche im Rahmen eines Schadenersatzes führen können. Zum anderen aber auch, dass der Schaden nicht unbedingt materiell bezifferbar sein muss, sondern auch immaterieller Natur sein kann. Und natürlich, dass ein solcher Schaden durchaus recht unterschiedlich bewertet werden kann.

Fazit für meine Datenschutz-Kunden

- Bitte nehmen Sie Meldungen über unrechtmäßig verarbeitete Daten ernst. Vertagen Sie erforderliche Korrekturen nicht. Im genannten Fall war es dem Verantwortlichen eventuell nicht bewusst, dass die Korrektur auf der Internet-Präsenz nicht bis zur nächsten geplanten Revision derselben verschoben werden darf.
- Prüfen Sie ihre Prozesse auf Lücken, insbesondere was erforderliche Datenlöschungen von ansonsten wenig beachteten Datengräbern anbelangt. Für den konkreten Fall würde ich vorschlagen, die Löschung von personenbezogenen Daten auf der Internet-Präsenz in die von mir vielfach empfohlene "Checkliste für den Austritt von Mitarbeitern" aufzunehmen.

Erinnerung zur Löschung von pandemiebedingten Aufzeichnungen

Nun aber zum zweiten Thema: Während der Hochzeiten der Corona-Maßnahmen wurden von vielen Verantwortlichen zusätzliche personenbezogene Daten erhoben, z. B. wer zu welchem Zeitpunkt das Unternehmen oder einen Betriebsteil betreten hat, welchen Status der Betroffene innehatte (Einhaltung der 2G- / 3G-Regeln), wer an Corona erkrankt war und zu wem der Erkrankte unmittelbar vor der Erkrankung räumlichen Kontakt hatte. Viele der von Behördenseite an Verantwortliche gestellten Anforderungen waren zu dieser Zeit datenschutzrechtlich auf eher wackeligen Füßen gestanden, fehlte doch häufig die direkte Rechtsgrundlage. Auf meine Nachfrage beim Bayerischen Landesamt für Datenschutzaufsicht, wie der Begriff "rechtliche Verpflichtung" im Art. 6 Abs. 1 c EU-DSGVO auszulegen sei, erhielt ich im April 2020 die folgende Antwort "... Wir verstehen Erwägungsgrund 45 so, dass es sich um eine im Unionsrecht oder in deutschen Gesetzen befindliche Vorschrift handeln muss. ..." Die Anordnung einer Verwaltung würde es dementsprechend nicht erlauben, sich auf diesen Rechtsgrund zu beziehen. Vielleicht hätte man sich als Verantwortlicher auch eher auf Art. 6 Abs. 1 f EU-DSGVO berufen können, nämlich dem berechtigten Interesse des Verantwortlichen, Ärger mit Strafverfolgungsbehörden und Aufsichtsämtern zu vermeiden. Egal, die meisten der Corona-Regeln sind entfallen und damit auch jegliche Rechtsgrundlage für eine weitere Verarbeitung der diesbezüglich erhobenen Daten.

Ich empfehle daher dringend, eventuell noch vorhandene "Corona-Aufzeichnungen" (gleich ob in analogen oder digitalen Formaten) unverzüglich zu löschen, sofern man nicht zu einer der wenigen Einrichtungen gehört, für die noch Aufzeichnungspflichten bestehen. Aber auch dort gilt natürlich, dass die Speicherung der Daten zeitlich zu befristen ist.

München, 2022-05-23

Volker Baron

- 1) Für die beiden großen Kirchen in Deutschland gelten jeweils eigene Datenschutzgesetze (Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland - DSG-EKD bzw. Gesetz über den Kirchlichen Datenschutz - KDG). Dort sind die Höchstgrenzen für zu verhängende Bußgelder auf 500.000 EUR festgelegt.