

Nr. 07 / 2021



Newsletter Datenschutz

In dieser Ausgabe:

Facebook und WhatsApp: EDSA stoppt Hamburger Datenschützer	2
Ergänzende Prüfungen und Maßnahmen trotz neuer EU-Standardvertragsklauseln für Datenexporte nötig	2
Reichweite des Auskunftsanspruches	3
Verwertung verdeckt aufgenommener Überwachungsvideos bei Diebstahlsvorwurf ..	3
Kein Einsichtsrecht des Betriebsrats in die elektronische Personalakte ohne Zustimmung der Arbeitnehmer	4
VERANSTALTUNGEN	6
„Controlling digital – Digitale Finanzbuchführung als Zukunftsmodell“	6
„Betriebsrentenanpassungsgesetz“	6

Facebook und WhatsApp: EDSA stoppt Hamburger Datenschützer

Der Europäische Datenschutzausschuss (EDSA) hat den Antrag des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) abgelehnt, endgültige Maßnahmen zu verhängen, um einen Datenaustausch zwischen WhatsApp und Facebook zu verhindern. Er bewertete diese Frage als nicht dringlich.

Der EDSA stellte zwar erhebliche Widersprüche zwischen den Informationen fest, mit denen einerseits die WhatsApp-Nutzern über weitreichende Verwendungen ihrer Daten durch Facebook informiert werden, und andererseits den Zusagen der Unternehmen gegenüber Datenschutzaufsichtsbehörden, dies gleichwohl (noch) nicht zu tun. Der EDSA meldete zudem erhebliche Zweifel an der Rechtsgrundlage an, auf die sich Facebook bei der Nutzung der WhatsApp-Daten für eigene oder gemeinsame Verarbeitungen stützen möchte. Er greift damit wesentliche Teile der Argumentation des HmbBfDI auf.

Trotz dieser Feststellungen hat sich der EDSA dazu entschlossen, die federführende irische Datenschutzaufsichtsbehörde (IDPC) anzuhalten, eine Prüfung vorzunehmen. Diese soll die tatsächlichen Verarbeitungsprozesse bei Facebook in Bezug auf WhatsApp-Daten und die Frage der möglichen Rechtsgrundlage umfassen, insbesondere des überwiegenden berechtigten Interesses im Sinne von Art. 6 Abs. 1 f) DSGVO. Eine Frist wurde der IDPC hierfür nicht gesetzt.

Quelle: PM des HmbBfDI vom 15. Juli 2021

Ergänzende Prüfungen und Maßnahmen trotz neuer EU-Standardvertragsklauseln für Datenexporte nötig

Die EU-Kommission hat [neue Standardvertragsklauseln](#) erlassen, die eine rechtskonforme Übermittlung personenbezogener Daten in Drittländer ermöglichen sollen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist wie auch der Europäische Datenschutzausschuss (EDSA) darauf hin, dass auch bei Verwendung der neuen EU-Standardvertragsklauseln eine Prüfung der Rechtslage im Drittland und zusätzlicher ergänzender Maßnahmen erforderlich ist.

Für die Prüfung der Rechtslage im Drittland und der ergänzenden Maßnahmen können Verantwortliche die „[Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten](#)“ heranziehen.

An der beschriebenen Situation und den sich daraus ergebenden Verpflichtungen hat sich durch die neuen Standardvertragsklauseln nichts geändert. Diese regeln die bisher nur aus der Rechtsprechung des EuGH folgenden Anforderungen nun vielmehr ausdrücklich. Die EU-Kommission und der EDSA haben die neuen Standardvertragsklauseln und die Empfehlungen 01/2020 bewusst aufeinander abgestimmt. Das heißt, auch bei Verwendung der neuen Klauseln muss der Datenexporteur die Rechtslage und -praxis des Drittlands prüfen und ggf. zusätzliche Schutzmaßnahmen ergreifen bzw., wenn dies nicht gelingt, von der Übermittlung Abstand nehmen.

Unternehmen und andere Akteure, die personenbezogene Daten in Drittländer übermitteln, müssen gegenüber der Aufsichtsbehörde nachweisen können, dass sie die hier dargestellte Prüfung zum Schutzniveau im Drittland im Einzelfall durchgeführt haben und zu einem positiven Ergebnis gekommen sind. [Die deutschen Aufsichtsbehörden haben mit Beratungen und Prüfungen dazu begonnen](#), ob und wie die Anforderungen des „Schrems II“-Urteils eingehalten werden.

Quelle: PM des UDZ Saarland vom 22. Juni 2021

Reichweite des Auskunftsanspruches

Verlangt ein Kunde Auskunft darüber, welche personenbezogene Daten ein Unternehmen von ihnen verarbeitet oder gespeichert hat, muss dieses über sämtliche Vorgänge und Verteiler informieren, die diese Daten enthalten. Dies hat der BGH in einem aktuellen Urteil entschieden.

Unternehmen, die personenbezogene Daten speichern oder bearbeiten, sind verpflichtet, den betroffenen Personen über die Art und Weise der Verarbeitung oder Speicherung, auf Verlangen Auskunft zu geben. In einer aktuellen Entscheidung hat sich der BGH mit der Reichweite des Auskunftsanspruchs auseinandergesetzt. Er ist der Ansicht, dass vom Auskunftsanspruch „alle Arten von Informationen“, also auch persönliche Daten umfasst sind, die lediglich im Zusammenhang mit internen Vorgängen stehen. Irrelevant für den Auskunftsanspruch ist, ob der Betroffene bereits Kenntnis von den Unterlagen hat.

In dem zu entscheidenden Fall schloss der Kläger 1997 eine Lebensversicherung ab. Er widersprach 2016 erfolglos dem Zustandekommen des Vertrags. Im Anschluss machte der Kläger gegenüber der Versicherung sein Recht auf Auskunft geltend und forderte diese auf, ihm mitzuteilen, welche personenbezogenen Daten die Versicherung über ihn speichert und verarbeitet. Daraufhin erhielt der Kläger eine Datenübersicht, welche er für unvollständig erachtete, weil unter anderem interne Aktenvermerke und der wechselseitige Schriftverkehr fehlten.

Der BGH schloss sich der Auffassung des Klägers weitestgehend an. Das Gericht versteht den Begriff der personenbezogenen Daten weit und sieht hiervon sämtliche Informationen umfasst, die auf Grund ihres Inhalts, Zwecks oder ihrer Auswirkungen mit einer Person im Zusammenhang stehen, also auch die Korrespondenz einschließlich E-Mails, interne Telefon- und Gesprächsnotizen sowie sonstige interne Vermerke.

BGH, Urteil vom 15. Juni 2021, VI ZR 576/19

Verwertung verdeckt aufgenommener Überwachungsvideos bei Diebstahlsvorwurf

Das LAG Nürnberg hat entschieden, dass der Einsatz einer verdeckten Kamera zur Aufklärung vor Straftaten rechtmäßig sein kann und damit im Prozess verwertet werden kann. Voraussetzung ist, dass der Arbeitgeber vor der Installation der verdeckten Videokamera die ihm zur Verfügung stehenden Möglichkeiten ausgeschöpft hat, den möglichen Täterkreis mit entsprechenden Verdachtstatsachen einzugrenzen.

Der Beklagte, ein Großhandelslager für Obst und Gemüse, Frische- und Trockensortiment wie Getränke und Spirituosen, hatte in der Vergangenheit Warenschwund zu beklagen. Wegen des Schwundes an Spirituosen waren Mitarbeiter beauftragt worden, die Gänge im Bereich des Trockensortiments zu kontrollieren, ob sich dort jemand unberechtigt aufhalte. Ferner war eine versteckte Kamera angebracht worden, die den Gang mit den Spirituosen im Aufnahmebereich der Kameralinse hatte. Diese wurde eingeschaltet in den Zeiten, in denen im Trockensortiment nicht gearbeitet wurde. Die Kamera war mit einem Bewegungsmelder versehen und fertigte nur Aufzeichnungen bei Bewegungen im Aufnahmebereich.

Als zwei Schichtarbeiter bemerkten, dass der an dem Tag im Frischebereich arbeitende Kläger mit einem Kollegen aus dem Trockenbereich kam, in dem zu diesem Zeitpunkt nicht gearbeitet wurde und das Licht ausgeschaltet war, prüften sie den Bestand und stellten das Fehlen zweier Flaschen Jägermeister fest. Auf den Videoaufnahmen war zu erkennen, dass sich der Kläger im betreffenden Bereich bückte. Der Kläger wurde mit dem Vorwurf konfrontiert, er habe sich Jägermeisterfläschchen angeeignet. Die Videoaufzeichnungen wurden dem Kläger nicht gezeigt. Er stritt den Vorwurf ab. Danach wurde der Kläger heimgeschickt und später fristlos gekündigt.

Das Arbeitsgericht hat der Kündigungsschutzklage stattgegeben. Die Berufung der Beklagten hatte keinen Erfolg. Die Beklagte konnte im Prozess nicht beweisen, dass ein Kündigungsgrund vorliegt. Die von der Beklagten vorgelegten Videoaufzeichnungen und Screenshots durften aufgrund des Widerspruchs des Klägers nicht verwertet werden. Der Verwertung stand das allgemeine Persönlichkeitsrecht des Klägers entgegen, da der Verhältnismäßigkeitsgrundsatz nicht gewahrt wurde. Auch wenn die Verarbeitung gegen die Bestimmungen des Datenschutzes verstößt, bedeutet dies zwar nicht automatisch, dass die Daten nicht im gerichtlichen Verfahren verwertet werden dürfen. Nach der Rechtsprechung des BAG dürfen die Bilder im gerichtlichen Verfahren trotzdem verwertet werden, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachttes ergebnislos ausgeschöpft sind, die verdeckte Kameraüberwachung damit das praktisch einzig verbleibende Mittel darstellt.

Vorliegend konnte die Beklagte nicht darlegen, dass sie vor der Installation und Inbetriebnahme der Überwachungskamera andere, nicht in das Persönlichkeitsrecht der Arbeitnehmer eingreifende Mittel zur Aufklärung des Verdachttes des Diebstahles von Spirituosen ausgeschöpft hat und die Kameraüberwachung das praktisch einzig verbliebene Mittel zur Aufklärung der Täterschaft war. Ein milderer Mittel wäre zum Beispiel gewesen, die An- und Abwesenheitszeiten abzugleichen, um den Kreis der Verdächtigten weiter einzugrenzen.

Kein Einsichtsrecht des Betriebsrats in die elektronische Personalakte ohne Zustimmung der Arbeitnehmer

Ein permanenter Lesezugriff des Betriebsrats auf die elektronischen Personalakten der Arbeitnehmer zu Kontrollzwecken ist unzulässig, da hiermit unverhältnismäßig in das allgemeine Persönlichkeitsrecht der Arbeitnehmer eingegriffen wird. Dies hat das LAG Düsseldorf entschieden.

Im vorliegenden Fall wurde in einer Gesamtbetriebsvereinbarung eines Telekommunikationsanbieters festgelegt, dass der Gesamtbetriebsratsvorsitzende und der örtliche Betriebsratsvorsitzende permanenten Zugriff auf (fast) alle elektronischen Personalakten erhält. Die Arbeitgeberin verwehrt der Betriebsratsseite diesen Zugriff. Der Gesamtbetriebsrat hat daraufhin ein Verfahren vor dem Arbeitsgericht Düsseldorf eingeleitet, mit dem er einen Anspruch auf Einsicht in die elektronischen Personalakten durchsetzen will.

Das Arbeitsgericht hat die Anträge ebenso wie das Landesarbeitsgericht zurückgewiesen. Die Bestimmung in der Gesamtbetriebsvereinbarung sind unwirksam. Das generelle Einsichtsrecht der Betriebsratsvorsitzenden in die elektronische Personalakte der Arbeitnehmer, ohne Zustimmung des Arbeitnehmers, verletzt ihn in seinem allgemeinen Persönlichkeitsrecht. Ein derart weites Einsichtsrecht des Betriebsrates ist weder geeignet noch erforderlich, um den Arbeitgeber hinsichtlich der Einhaltung der rechtlichen Bestimmungen zu kontrollieren. Dies gilt insbesondere auch deshalb, weil dem Betriebsrat anderen spezifische Kontrollrechte eingeräumt wurden.

LAG Düsseldorf, Beschluss vom 23. Juni 2020, 3TaBV65/19

VERANSTALTUNGEN

„Controlling digital – Digitale Finanzbuchführung als Zukunftsmodell“ Dienstag, 2. November 2021, 17.00 bis 19.00 Uhr, Onlineveranstaltung

Referent: Herr Guido Badjura, DATEV eG, Düsseldorf

Gemeinschaftsveranstaltung der IHK Saarland, der Steuerberaterkammer Saarland und der Datev eG

Anmeldungen bis 01.11.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

„Betriebsrentenanpassungsgesetz“ Donnerstag, 4. November 2021, 14.00 bis 16.00 Uhr, Onlineveranstaltung

Referent: Herr Rechtsanwalt Dr. Kai Hüther, Fachanwalt für Arbeitsrecht, Kanzlei Rapräger, Saarbrücken

Anmeldungen bis 03.11.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

Verantwortlich und Redaktion:

Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß

Tel.: (0681) 9520-600

Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines

Tel.: (0681) 9520-640

Fax: (0681) 9520-690

E-Mail: kim.pleines@saarland.ihk.de

Impressum:

IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dr. Frank Thomé, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, USt-IdNr.: DE 138117020