

Fachgebiet: Consulting

Dirk Hellmann
DigitEX, Datenschutzbeauftragter

Schadenersatz für unzureichende DSGVO-Auskunft

Eine unzureichende Daten Auskunft des Arbeitgebers kann schwere wirtschaftliche Folgen für den Arbeitgeber haben.

Es ist einer der ersten Fälle zur DSGVO-Thematik, der bei den Gerichten angekommen ist: Das Arbeitsgericht Düsseldorf hatte sich mit der Frage zu befassen, ob und inwieweit ein Arbeitnehmer wegen unvollständiger Auskünfte nach Art. 15 DSGVO gegenüber seinem Arbeitgeber einen Anspruch auf Schadenersatz nach Art. 82 Abs. 1 DSGVO hat.

Der Kläger war bis Januar 2018 bei der Beklagten zu einem Gehalt von 12.000 EUR brutto pro Monat beschäftigt. Im November verlangte der Kläger klageweise Auskunft zur Verarbeitung seiner personenbezogenen Daten. Die Beklagte überreichte daraufhin die gewünschten Unterlagen, sowie die Zugangsdaten, damit der Kläger weitere personenbezo-

genen Daten auf einer Internetseite abrufen konnte.

Die zur Verfügung gestellten Daten durch den Arbeitgeber waren jedoch unvollständig, sodass der Kläger dafür Entschädigung verlangte, „unter anderem wegen verspäteter und unvollständiger Auskunftserteilung in Höhe von 12 Brutto-Monatsgehältern.“

Erteilt werden muss Auskunft zu Daten-Kategorien und Zwecken der Verarbeitung.

Mit den Anträgen zu den Auskünften ging es während des Verfahrens hin und her. Viele wurden gestellt, nach richterlichen Hinweisen konkretisiert, umgestellt oder zurückgenommen und per Urteil teilweise abgewiesen. Am Ende sprach das Arbeitsgericht Düsseldorf dem klagenden Ex-Mitarbeiter eine Auskunft zu den Zwecken, für die die personenbezogenen Daten verarbeitet wurden, sowie zu den Kategorien der verarbeiteten Daten zu.

Die Mitteilung zur Datenverarbeitung muss präzise, transparent, verständlich und in leicht zugänglicher Form in klarer, einfacher Sprache erfolgen (Art. 12 Abs.1 S.1 DSGVO). Pauschalitäten oder Phrasen, wie es das beklagte Unternehmen hier versuchte, reichen nicht. Die Angaben müssen vollständig, konkret und detailliert sein. Auch Verweise auf Anlagen genügen den Anforderungen nicht.

Datenkopien nur bei vertretbarem Aufwand

Der Kläger verlangte außerdem Kopien seiner verarbeiteten Daten, soweit sie auf Endgeräten und in Datensammlungen von Vorgesetzten und Kollegen vorhanden waren, also beispielsweise in Notebooks oder E-Mail-Postfächern. Diesem Begehren schob das Arbeitsgericht im vorliegenden Fall einen Riegel vor, weil der nötige Aufwand schlicht in zu grobem Missverhältnis zum Leistungsinteresse des Klägers stand.

Schaden mit 5.000 Euro bewertet

Nachdem festgestellt wurde, dass die Auskunftspflicht verletzt ist, ging es um die Höhe des immateriellen Schadenersatzanspruchs (Art. 82 DSGVO). Dazu gibt das Gesetz nichts vor, außer dass der Schaden vollständig und wirksam ersetzt wird und

Fortsetzung

Schadenersatz für unzureichende DSGVO-Auskunft

Verstöße effektiv sanktioniert werden sollen. Von den beantragten 140.000 wurden dem Kläger letztendlich 5.000 Euro zugesprochen.

Die Kammer setzte dabei für die ersten zwei Monate der Verspätung jeweils 500 €, für die weiteren etwa drei Monate jeweils 1.000 € und für die beiden inhaltlichen Mängel der Auskunft jeweils 500 € an. Die Kammer sah keinen Anlass, sich am Gehalt des Klägers zu orientieren.

Fazit

Die Verurteilung zur Zahlung von Schadenersatz in dieser Höhe wirkt zunächst abschreckend und trifft nicht sofort auf Verständnis. Jedoch ist sie das exakte Resultat der unionsrechtlichen Vorgaben.

Falls weitere Gerichte den Ansichten des Arbeitsgerichts Düsseldorf folgen sollten, müssten sich Unternehmen künftig auf eine Vielzahl von Schadenersatzprozessen nach Art. 82 DSGVO einstellen. Eine extensive Auslegung von Art. 82 DSGVO könnte es für Kläger, Verbrauchernanwälte und Prozessfinanzierer lukrativ machen, immaterielle Schäden wegen tatsächlicher oder vermeintlicher DSGVO-Verstöße einzuklagen.

„Schrems II“ und die Auswirkungen auf den Beschäftigtendatenschutz

Ein kürzlich ergangenes Urteil des EuGH hält weiteren Handlungsbedarf für Arbeitgeber bereit. Jede Übermittlung von personenbezogenen Daten in Länder außerhalb der EU bedarf einer besonderen rechtlichen Absicherung.

Lagern Unternehmen beispielsweise Aufgaben an externe Dienstleister in Drittstaaten aus, kommt es dabei häufig zur Übermittlung personenbezogener Daten. Auch in Konzernstrukturen kann die Übermittlung von personenbezogenen Beschäftigtendaten in Drittstaaten notwendig sein, wenn eine Konzerngesellschaft Dienstleistungen für eine andere erbringt.

Bislang konnten sich Unternehmen bei Übermittlungen in die USA auf eine Zertifizierung nach dem „EU/US Privacy Shield“ des Datenempfängers stützen.

Der Europäische Gerichtshof hat jedoch durch Urteil vom 16. Juli 2020 (C-311/18, „Schrems II“) entschieden, dass diese Zertifizierung kein angemessenes Schutzniveau bietet. Das bedeutet, dass jede Übermittlung von personenbezogenen Beschäftigten-

daten in die USA nunmehr unzulässig ist, sofern sie ausschließlich auf dem Privacy Shield basiert.

Wenn Sie vermeiden wollen, in unzulässiger Art und Weise personenbezogene Beschäftigtendaten an Konzerngesellschaften oder externe Dienstleister in die USA zu übermitteln, sollten Sie zügig überprüfen, mit welchem Instrument der Datentransfer derzeit datenschutzrechtlich abgesichert wird.

Falls sich die Übermittlung ausschließlich auf das „EU/US Privacy Shield“ stützt, sollte dringend geprüft werden, ob für den Zweck nicht auch ein anderer Dienstleister eingesetzt werden kann, bei dem die Transferproblematik nicht besteht. Alternativ können mit bestehenden Dienstleistern in bestimmten Fällen auch Verträge mit zusätzlichen Garantien abgeschlossen werden.

Auch wenn die Datenschutzbehörden sicherlich eine gewisse Übergangsphase gewähren dürften, sind mittelfristig erhebliche Bußgelder zu befürchten, sofern der Drittlandtransfer nicht datenschutzrechtlich abgesichert ist.