www.jusletter-it.eu

Jurius

Auftragsdatenverarbeitung ohne richtigen Vertrag kann teuer werden

Those who have others work for them with personal data, have to conclude a rather detailed contract by operation of law. If such a contract is not or insufficiently concluded, a fine can be imposed. The Bavarian Data Protection Authority (BayLDA) has recently imposed a fine running into tens of thousands in the event of inadequate award of contract. (ah)

Category: News
Region: Germany
Field of law: Data Protection; Data Security

Citation: Jurius, Auftragsdatenverarbeitung ohne richtigen Vertrag kann teuer werden, in: Jusletter IT 24 September 2015

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

[Rz 1] Wer einen externen Dienstleister als so genannten Auftragsdatenverarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, muss mit diesem einen schriftlichen Vertrag abschließen. Das Gesetz schreibt eine Reihe von Einzelheiten vor, die zum Schutz der personenbezogenen Daten darin ausdrücklich festgelegt werden müssen. Von besonderer Bedeutung sind dabei die technischen und organisatorischen Maßnahmen (Datensicherheitsmaßnahmen), die der Auftragsdatenverarbeiter zum Schutz der Daten treffen muss. Diese Maßnahmen müssen im schriftlichen Auftrag konkret und spezifisch festgelegt werden. Fehlen konkrete Festlegungen hierzu, stellt dies eine Ordnungswidrigkeit dar, die mit Geldbuße von bis zu 50.000.– €geahndet werden kann.

[Rz 2] Das BayLDA hat kürzlich gegen ein Unternehmen eine Geldbuße in fünfstelliger Höhe festgesetzt. Das Unternehmen hatte in seinen schriftlichen Aufträgen mit mehreren Auftragsdatenverarbeitern keine konkreten technisch-organisatorischen Maßnahmen zum Schutz der Daten festgelegt. Stattdessen enthielten die Aufträge nur einige wenige pauschale Aussagen und Wiederholungen des Gesetzestextes. Dies reicht keinesfalls aus. Denn die datenschutzrechtliche Verantwortung trägt auch im Falle der Einschaltung von Auftragsdatenverarbeitern nach wie vor der Auftraggeber. Dieser muss daher beurteilen können, ob der Auftragsdatenverarbeiter in der Lage ist, für die Sicherheit der Daten zu sorgen. Auch muss der Auftraggeber die Einhaltung der technisch-organisatorischen Maßnahmen bei seinem Auftragnehmer kontrollieren. Hierfür ist es unerlässlich, dass die beim Auftragsdatenverarbeiter zum Schutz der Daten zu treffenden technisch-organisatorischen Maßnahmen in dem abzuschließenden schriftlichen Auftrag spezifisch festgelegt werden. Nur so kann der Auftraggeber beurteilen, ob die personenbezogenen Daten bei seinem Auftragnehmer z.B. gegen Auslesen oder Kopieren durch Unbefugte, gegen Verfälschung oder sonstige unberechtigte Abänderung oder gegen zufällige Zerstörung geschützt sind.

[Rz 3] Welche vertraglichen Festlegungen zu den technisch-organisatorischen Maßnahmen getroffen werden müssen, kann nicht pauschal beantwortet werden, sondern richtet sich nach dem Datensicherheitskonzept des jeweiligen Dienstleisters und den von diesem zum Einsatz gebrachten spezifischen Datenverarbeitungssystemen. Den gesetzlichen Maßstab für die festzulegenden technisch-organisatorischen Maßnahmen bildet jedenfalls die Anlage zu § 9 BDSG, die Maßnahmen in den Bereichen Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle verlangt. Grundsätzlich muss der schriftliche Auftrag daher spezifische Festlegungen zu diesen Fragen enthalten.

Quelle: Medienmitteilung des Bayerischen Landesamtes Datenschutzaufsicht vom 20. August 2015

Weitere Informationen:

- Bayerisches Landesamt für Datenschutzaufsicht – Informationsblatt «Auftragsdatenverarbeitung nach § 11 BDSG»