



Ansbach, den 20. August 2015

Pressemitteilung

„Auftragsdatenverarbeitung ohne richtigen Vertrag kann teuer werden“

Wer andere für sich mit personenbezogenen Daten arbeiten lässt, muss darüber Kraft Gesetzes einen ziemlich detaillierten Vertrag schließen. Wird so ein Vertrag nicht oder unzureichend abgeschlossen, droht ein Bußgeld. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat kürzlich im Fall einer unzureichenden Auftragserteilung eine Geldbuße in fünfstelliger Höhe festgesetzt.

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.

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.

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.

„Augen auf beim Einbinden von Dienstleistern. Jeder Auftraggeber muss wissen und gegebenenfalls auch prüfen, was sein Auftragnehmer mit den Daten macht.“, appelliert Thomas Kranig, der Präsident des BayLDA an die Auftraggeber. *„Die Datensicherheitsmaßnahmen müssen konkret und spezifisch im Vertrag festgelegt werden. Unspezifische oder pauschale Beschreibungen reichen nicht aus. Wir werden auch künftig in geeigneten Fällen Verstöße in diesem Bereich mit Geldbußen ahnden.“*

Nähere Informationen zu den inhaltlichen Anforderungen an die Erteilung von Aufträgen zur Auftragsdatenverarbeitung finden sich in einem Merkblatt des BayLDA. Dieses Informationsblatt ist auf der Homepage des BayLDA [abrufbar](#).



Thomas Kranig
Präsident