23.05.2013

Hinweise

zur biometrischen Datenerfassung am Arbeitsplatz

In der Vergangenheit werden zunehmend Zeiterfassungssysteme angeboten, die biometrische Daten der Beschäftigten nutzen. Insbesondere sogenannte Fingerprint-Zeiterfassungssysteme kommen hierbei zur Anwendung. Die Erfassung der Arbeitszeit von ArbeitnehmerInnen als Grundlage zur Berechnung von Löhnen und Gehältern als auch zur Ausübung einer Arbeitszeitkontrolle ist ein legitimes Recht von Unternehmen. Eine ordnungsgemäße Erfassung der Arbeitszeit liegt aber ebenso im rechtlichen Interesse der Beschäftigten selbst.
Die Verwendung eines Fingerprint-Zeiterfassungssystems berührt in erheblichem Maße datenschutzrechtliche Probleme. Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit weist deshalb auf folgendes hin:

1. Die Erhebung, Speicherung, Übermittlung und Nutzung biometrischer Daten stellt grundsätzlich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der ArbeitnehmerInnen dar. Er ist gemäß § 4 Abs. 1 Satz 1 BDSG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Biometrische Daten gelten dabei als besonders sensible Daten, die einer besonderen Schutzbedürftigkeit unterliegen.
2. Es existieren für die ArbeitnehmerInnen weit weniger in das Recht auf informationelle Selbstbestimmung eingreifende und dem Grundsatz der Datensparsamkeit nach § 3 a Bundesdatenschutzgesetz (BDSG) gerecht werdende technische wie organisatorische Möglichkeiten, die geeignet sind, die Arbeitszeit zu erfassen und dabei ohne die Verwendung biometrischer Daten auskommen.

Postanschrift : Postfach 900455
99107 Erfurt
Dienstgebäude : Jürgen-Fuchs-Str. 1
99096 Erfurt
Telefon: 0361 37-71900
Telefax: 0361 37-71904
E-Mail*: poststel-
le@datenschutz.thueringen.de
Internet: www.thueringen.de/datenschutz

3. Allein die geringere, aber auch nicht auszuschließende Betrugsanfälligkeit, Arbeitszeiten zu manipulieren, führt im Rahmen einer Verhältnismäßigkeitsprüfung nicht zu einer anzunehmenden Erforderlichkeit der Verwendung biometrischer Daten zur Arbeitszeiterfassung. Es kann regelmäßig nicht davon ausgegangen werden, dass ArbeitnehmerInnen sich rechtswidrig verhalten. Im Falle festgestellter Falschangaben von Arbeitszeiten stehen dem Arbeitsgeber genügend Mitel zur Vertretung eigener Interessen (z. B. strafrechtliche Verfolgung wegen Betruges gem. § 263 StGB und außerordentliche Kündigung) zur Verfügung.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auch biometrischer Daten, ist gem. § 4 Abs. 1 BDSG unter anderem dann zulässig, wenn der von der Datenverarbeitung Betroffene einwilligt. Die Einwilligung ist aber nur unter den Voraussetzungen des § 4 a BDSG wirksam, d. h. wenn diese schriftlich und tatsächlich freiwillig abgegeben und der Betroffene auf die Folgen einer verweigerten Einwilligung hingewiesen wird. Insbesondere in bestehenden Abhängigkeitsverhältnissen, wie im Rahmen arbeitsvertraglicher Beziehungen, ist die Frage der Freiwilligkeit regelmäßig kritisch zu hinterfragen. Insbesondere müssen die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten umfassend informiert werden. Außerdem muss es eine tatsächliche Alternative zu der biometrischen Zeiterfassung geben, sodass der betroffene Arbeitnehmer ein Wahlrecht hat.
In Unternehmen mit einem Betriebsrat unterliegt die Verwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (wie z.B. automatisierte Arbeitszeiterfassungssysteme), gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz der Mitbestimmung des Betriebsrates. .

Die Verwendung von Fingerprint-Zeiterfassungssystemen zur Authentifizierung kann nur unter folgenden Gesichtspunkten zulässig sein, wenn das Verfahren Zutritts- bzw. Zugriffsrechte zu besonders sicherheitsrelevanten bzw. schutzbedürftigen Bereichen sicherstellen soll. Vor Einführung ist daher das Verfahren einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung zu unterziehen. Unter **der Voraussetzung der Erforderlichkeit** ist eine biometrische Zutritts- oder Zugriffskontrolle dann zulässig, wenn

1. die Daten auslesesicher gegen unbefugten Zugriff geschützt sind und eine zweckentfremdende Nutzung der biometrischen Daten für andere als den ursprünglich geplanten Zweck zur Identitätsfeststellung im Zusammenhang mit Zutritts- bzw. Zugriffsrechten durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist,
2. die Daten dem Stand der Technik verschlüsselt übertragen und gespeichert werden,
3. eine vollständige Transparenz für die von der Datenspeicherung Betroffenen über die Datenerhebung und Datenverwendung hergestellt ist. Die Betroffenen müssen jederzeit darüber in Kenntnis sein, wann und wer Zugriff auf die Daten hat und zu welchem konkreten Zweck der jeweilige Datenzugriff erfolgt. Das Verfahren ist daher vollständig und umfassend in einer Vereinbarung o. ä. zu beschreiben, die jedem Beschäftigten zugänglich sein muss,
4. die technischen und organisatorischen Sicherheitsvorkehrungen zum Ausschluss einer unbefugten Verarbeitung, Nutzung und Speicherung, z. B. auch durch eine Übersicht über bestehende Zugriffsberechtigungen, dokumentiert und den Beschäftigten zugänglich sind,
5. die Speicherung der Fingerabdrücke in datensparsamen Templates erfolgt und
6. biometrische Verfahren, die der Verifikation dienen, mit einer dezentralen Datenspeicherung betrieben werden.

Der TLfDI weist darauf hin, dass die biometrische Zeiterfassung einer Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten bedarf, weil sie besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist.