Maximilian Schnebbe

Kündigung

Die Beendigung eines Arbeitsverhältnisses stellt Unternehmen regelmäßig vor verschiedene Herausforderungen. Unabhängig davon, ob es sich um eine einseitige oder einvernehmliche Beendigung handelt, werden dabei regelmäßig auch Beschäftigtendaten verarbeitet. Mithin ist bei einer Kündigung auch das Datenschutzrecht zu beachten und ggf. der Datenschutzbeauftragte frühzeitig in den Kündigungsprozess mit einzubeziehen. Gerade bei Verdachtsfällen bezüglich einer Pflichtverletzung oder Straftat des Arbeitnehmers stellt sich die Frage, ob und wie Daten verarbeitet werden dürfen, um diesen Missstand aufzuklären und arbeitsrechtliche Konsequenzen zu ziehen.

Die Grundlagen

Der Beschäftigtendatenschutz ist aufgrund der Öffnungsklausel in Art. 88 DS-GVO weitestgehend dem nationalen Gesetzgeber überantwortet. Davon hat der deutsche Gesetzgeber Gebrauch gemacht und in § 26 BDSG (n. F.) die Verarbeitung von Beschäftigtendaten geregelt. Gem. § 26 Abs. 1 BDSG dürfen personenbezogene Daten von Beschäftigten verarbeitet werden, soweit dies für die Beendigung des Beschäftigungsverhältnisses erforderlich ist. Wann genau von der Erforderlichkeit der Verarbeitung ausgegangen werden kann, ist der Norm selbst nicht zu entnehmen. Unstreitig ist die Erforderlichkeit bei einer Verarbeitung von Stammdaten zu bejahen. So sind Beschäftigungsdauer und Gehaltshöhe erforderlich, um die Kündigungsfrist oder die Höhe der Abfindung zu berechnen. Auch ist eine Verwendung bestimmter Beschäftigtendaten für die Kündigung zulässig, sofern der Arbeitgeber diese zur Einhaltung seiner gesetzlichen Pflichten benötigt. Zu denken ist beispielsweise an die betriebsbedingte Kündigung, bei welcher der Arbeitgeber gem. § 1 Abs. 3 S. 1 KSchG eine Sozialauswahl durchführen muss. Hierfür dürfen die notwendigen Daten verwendet werden. Dazu zählt insbesondere auch die Durchsicht der Personalakte im dafür gebotenen Umfang.

Die verhaltensbedingte Kündigung

Für die Beendigung des Arbeitsverhältnisses können nicht nur bereits gespeicherte Daten genutzt, sondern auch neue erhoben werden. Insbesondere bei der verhaltensbedingten Kündigung stellt sich hier die Frage, inwieweit Daten genutzt werden dürfen, die mit dem Ziel erhoben wurden, auf die Kündigung hinzuwirken, indem eine Straftat oder schwere Pflichtverletzung nachgewiesen werden soll. Das *BAG* hat in einer Reihe von Urteilen[1] einen Katalog mit Vorgaben entwickelt, wann und inwieweit Ermittlungs- und Überwachungsmaßnahmen zulässig sind, mithin prozessual als Beweismittel verwertet werden können. Danach muss die Überwachung erstens aufgrund eines einfachen, durch objektive Anhaltspunkte gestützten Verdachts einer Straftat oder erheblichen Pflichtverletzung durchgeführt worden sein. Zweitens muss die Überwachung erforderlich sein, d. h. es dürfen keine weniger einschneidenden Maßnahmen möglich sein, die denselben Erfolg herbeiführen würden. Drittens muss eine Verhältnismäßigkeitsprüfung stattfinden, bei der die Interessen des Arbeitgebers an einer Aufklärung und die Interessen des betroffenen Arbeitnehmers gegeneinander abgewogen werden. So ist beispielsweise der Einsatz eines *keyloggers* auf dem PC des Arbeitnehmers nicht datenschutzkonform, wenn die vorgeworfene Pflichtverletzung auch mittels einer Auswertung des Browserverlaufs nachzuweisen ist.[2]

Das neue Datenschutzrecht

Auch wenn das BAG diese Grundsätze noch vor Inkrafttreten der DS-GVO entwickelt hatte, dürfte sich an diesen auch nach Einführung des neuen Datenschutzrechts wenig ändern. Denn § 26 BDSG (n. F.) und § 32 BDSG (a. F.) gleichen sich weitestgehend.

Für die Verarbeitung zur Aufklärung einer *Straftat* enthält § 26 BDSG einen ausdrücklichen Erlaubnistatbestand in Satz 2. Für den Verdacht einer schwerwiegenden *Pflichtverletzung*, die keine Straftat darstellt, fehlt dagegen ein solcher. Demnach bestimmt sich im letzteren Fall die Erforderlichkeit einer Datenverarbeitung für die Beendigung des Arbeitsverhältnisses nach Satz 1.[3] Satz 2 entfaltet insoweit keine Sperrwirkung gegenüber Überwachungsmaßnahmen im Fall von Pflichtverletzungen, die keine Straftat sind. Dieser (zu § 32 BDSG a. F. vertretenen) Rechtsanwendung schließt sich ein Teil der Literatur auch für das neue Datenschutzrecht an.[4] Allerdings ist zu bedenken, dass eine heimliche Überwachung gegen Informationspflichten aus Art. 13 DS-GVO verstoßen könnte und insofern ein Unterschied zum alten Datenschutzrecht besteht. Wenngleich auch das alte Datenschutzrecht mit § 4 Abs. 3 BDSG (a.F.) eine vergleichbare Vorschrift kannte, können sich bei einem Verstoß die Geldstrafen der DS-GVO im Vergleich zum früheren BDSG geradezu drakonisch auswirken. Auch stehen die Informationspflichten des § 4 Abs. 3 BDSG (a. F.) denen aus Art. 13 DS-GVO um einiges nach.

Aufgrund der Ähnlichkeit von § 32 BDSG (a. F.) und § 26 BDSG (n. F.) wird das *BAG* an den von ihm entwickelten Grundsätzen zu Ermittlungsmaßnahmen festhalten. Allerdings muss diese Rechtsprechung auch vor dem *EuGH* Bestand haben. In jedem Fall aber bleibt es dabei: Die Überwachung eines Angestellten ist allenfalls bei einem konkreten Verdacht und nach einer umfassenden Interessenabwägung zulässig.

1 BAG Urt. v. 22.09.2016 – 2 AZR 848/15, NZA 2017, 112; Urt. v. 20.10.2016 – 2 AZR 395/15 , NZA 2017, 443; Urt. v. 22.07.2017 – 2 AZR 681/16, NZA 2017, 1327.

2 *Fuhlrott*, NZA 2017, 1308 (1309).

3 *Lingemann*, ArbRAktuell 2016, 532 (532).

4 Z.B. *Gräber/Nolden* in Paal/Pauly, DS-GVO BDSG, § 26 Rn. 21 ff.