9 Mitarbeiterscreenings

Möglichkeiten und Grenzen

Mitarbeiterscreenings werden in Unternehmen immer häufiger eingesetzt. Screenings sind Rasterfahndungen, bei denen verschiedene personenbezogene Daten der Mitarbeiter nach bestimmten Kriterien (Prüfraster) durchsucht werden. Mitarbeiter, deren Daten den Kriterien entsprechen, bleiben im Raster hängen, die anderen fallen durch. Die Screenings sollen der Aufdeckung von Betrug, Korruption oder Unterschlagung dienen.

Der Arbeitgeber hat aus verschiedenen gesetzlichen Normen heraus die Pflicht zur Durchführung von Kontrollmaßnahmen. Zu nennen wäre insbesondere als generelle Norm § 130 des Gesetzes über Ordnungswidrigkeiten (OwiG):

§ 130 OwiG
Gesetz über Ordnungswidrigkeiten

(1) Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.

(2) Betrieb oder Unternehmen im Sinne des Absatzes 1 ist auch das öffentliche Unternehmen.

(3) Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. Ist die Pflichtverletzung mit Geldbuße bedroht, so bestimmt sich das Höchstmaß der Geldbuße wegen der Aufsichtspflichtverletzung nach dem für die Pflichtverletzung angedrohten Höchstmaß der Geldbuße. Satz 2 gilt auch im Falle einer Pflichtverletzung, die gleichzeitig mit Strafe und Geldbuße bedroht ist, wenn das für die Pflichtverletzung angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.

9/1 Zulässigkeit von Mitarbeiterscreenings im Arbeitsverhältnis

Screenings verarbeiten personenbezogene Daten, daher sind sie nur zulässig, wenn die Betroffenen in die Verarbeitung einwilligen oder ein Gesetz die Verarbeitung erlaubt (§ 4 Abs. 1 BDSG).

Einwilligung kaum möglich

Eine rechtswirksame Einwilligung des Mitarbeiters in Kontrollmaßnahmen, die derart erheblich seine Persönlichkeitsrechte beeinträchtigen, wird für Mitarbeiterscreenings nicht zu erreichen sein. Auch wird die gebotene Freiwilligkeit der Einwilligung im Arbeitsverhältnis kaum herstellbar sein.

§ 32 BDSG als Erlaubnisnorm

Sind im Rahmen des Arbeitsverhältnisses bestimmte Kontrollmaßnahmen erforderlich, so ist § 32 BDSG die zuständige Erlaubnisnorm. Zu unterscheiden ist, ob das Mitarbeiterscreening präventiv, das heißt zur Vorbeugung von Betrugsfällen, oder repressiv, aufgrund eines konkreten Verdachts, erfolgen soll.

Präventive Kontrollmaßnahmen

Die Zulässigkeit einer präventiven Kontrolle im Rahmen des Arbeitsverhältnisses wäre nach § 32 Abs. 1 Satz 1 zu prüfen. Kontrollmaßnahmen gemäß § 32 Abs. 1 Satz 1 können beispielsweise zu folgenden Zwecken erfolgen:

- zur Leistungskontrolle
- zur Verhaltenskontrolle
- zur Verhinderung von Pflichtverletzungen
- zur Aufdeckung von Straftaten (ohne konkreten Tatverdacht)

Die gängigen Maßnahmen, die in Unternehmen zur präventiven Kontrolle eingesetzt werden, sind beispielsweise der Einsatz von Zeiterfassungssystemen, Taschenkontrollen oder – innerhalb der gebotenen Grenzen – auch die Videoüberwachung.

Ob allerdings das Datenscreening von Mitarbeitern als präventive Kontrollmaßnahme ebenfalls mit § 32 Abs. 1 Satz 1 BDSG begründet werden kann, ist umstritten. Weitgehend wird die Ansicht vertreten, dass ein Beschäftigtenverhältnis auch ohne präventives Mitarbeiterscreening möglich ist. Folgt man dieser Ansicht, dann ist § 32 Abs. 1 Satz 1 BDSG als mögliche Erlaubnisnorm für Mitarbeitersceenings nicht anwendbar.

Rahmenbedingungen von Mitarbeiterscreenings

Wird nach sorgfältiger Abwägung der berechtigten Interessen des Unternehmens und der Mitarbeiter aus Gründen der Compliance dennoch ein Mitarbeiterscreening ohne konkreten Tatverdacht durchgeführt, dann sind folgende Rahmenbedingungen zu beachten und vom Datenschutzbeauftragten in einer Vorabkontrolle zu prüfen:

- Der Grundsatz der Verhältnismäßigkeit ist zu beachten. Es ist zu prüfen, ob es statt des beabsichtigten Mitarbeiterscreenings kein milderes Mittel zur Erreichung des beabsichtigten Zwecks gibt

- Der Betriebsrat und der betriebliche Datenschutzbeauftragte sind in das Verfahren einzubeziehen.

- Das Screening muss stichprobenartig durchgeführt werden.

- Der vom Screening betroffene Mitarbeiterkreis ist möglichst klein zu halten.

- Das Verfahren ist transparent darzustellen. Die betroffenen Mitarbeiter sind vorher über das Screening zu informieren.

- Die Mitarbeiter, die vom Screening-Raster erfasst werden, befinden sich im Vorfeld eines Verdachts. Diese Verdachtsfälle sind umgehend zu klären. Die personenbezogenen Daten der nicht begründeten Verdachtsfälle sind unverzüglich zu löschen.

- Nach Abschluss des Screenings ist zu prüfen, ob das Screening zum beabsichtigten Ergebnis geführt hat. Stellt sich ein Screening im Nachhinein als nicht geeignet für den beabsichtigten Zweck heraus, so sind weitere derartige Screenings zu unterlassen.

- Die Übermittlung personenbezogener Mitarbeiterdaten an am Screening beteiligte Dritte ist zu vermeiden.

(Siehe auch 32. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen, 2009, 7.1 Beschäftigtenscreening als Unterschlagungsprüfung ohne Anlass.)

Zu prüfen ist, ob das Screening mit anonymisierten Mitarbeiterdaten durchgeführt werden kann. Dann wäre datenschutzrechtlich nichts dagegen einzuwenden, da keine personenbezogenen Daten betroffen sind.

Repressives Mitarbeiterscreening

Mitarbeiter-Kontrollmaßnahmen zur Aufdeckung von Straftaten bei konkretem Tatverdacht sind zulässig gemäß § 32 Abs. 1 Satz 2 BDSG. Diese Vorschrift erlaubt die Datenverarbeitung allerdings nur in sehr engen Grenzen. Sie verlangt, dass zur Aufdeckung von Straftaten die personenbezogenen Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Die Formulierung zielt auf konkrete Anhaltspunkte eines bestimmten Betroffenen ab. Ein unbestimmter Verdacht, dass irgendeine Person aus der Belegschaft eine Straftat begangen haben könnte, reicht für ein repressives Mitarbeiterscreening daher nicht aus.

Sei es bei der datenschutzrechtlichen Prüfung eines präventiven oder eines repressiven Mitarbeiterscreenings, es ist im jeden Fall sorgfältig der Grundsatz der Verhältnismäßigkeit zu beachten.

9/2 Screenings im Rahmen einer AEO-Zertifizierung

Möchten Unternehmen im internationalen Handel tätig sein, streben sie ein AEO-Zertifikat an. Das Zertifikat weist das Unternehmen als „Zugelassenen Wirtschaftsbeteiligten" (ZWB) oder englisch Authorized Economic Operator aus. Damit sind für das Unternehmen Vereinfachungen in Zollverfahren mit wirtschaftlicher Bedeutung verbunden. Um ein AEO-Zertifikat zu erhalten, sind umfangreiche Vorgaben einzuhalten.

Voraussetzungen einer AEO-Zertifizierung

- angemessene Einhaltung der Zollvorschriften in der Vergangenheit
- Nachweis der Zahlungsfähigkeit
- Nachweis einer zufriedenstellenden Buchhaltung
- Einhaltung geeigneter Sicherheitsstandards

Aufgrund der letztgenannten Voraussetzung für die AEO-Zertifizierung, der Einhaltung geeigneter Sicherheitsstandards, verlangen die Zollverwaltungen umfangreiche Mitarbeiterscreenings. Die Screenings werden meist regelmäßig und ohne konkreten Anlass wiederholt.

Erlaubnisnorm für AEO-Screenings?

Die Screenings im Rahmen der Einhaltung geeigneter Sicherheitsstandards für ein AEO-Zertifikat sind nicht mit § 32 Abs. 1 Satz 1 BDSG zu begründen. Denn das AEO-Zertifikat ist nicht unmittelbar zur Durchführung des Arbeitsverhältnisses notwendig. Auch § 32 Abs. 1 Satz 2 BDSG entfällt für eine Legitimierung, da bei AEO-Screenings in der Regel kein begründeter Tatverdacht für eine Straftat eines Mitarbeiters vorliegt.

Gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG könnte noch eine Abwägung zwischen dem berechtigten Interesse des Unternehmens, die Screenings zur Erfüllung eigener Geschäftszwecke durchzuführen, und den schutzwürdigen Interessen der Mitarbeiter infrage kommen.

Anwendung von § 28 BDSG umstritten

Es ist unter den Fachleuten und Juristen allerdings strittig, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG im Fall von Mitarbeiterscreenings zu AEO-Zertifizierung anwendbar sein kann. In Anbetracht dessen, dass eigentlich speziellere Vorschriften die allgemeinen Vorschriften überstimmen, wäre § 32 Abs. 1 Satz 1 BDSG die speziellere Norm.

Auch die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der Düsseldorfer Kreis, stehen Beschäftigtenscreenings im Rahmen von AEO-Zertifizierungen kritisch gegenüber. In einem Beschluss fordert der Düsseldorfer Kreis, „Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen", und weiter verlangt er, „die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten".

(Quelle: Beschluss des Düsseldorfer Kreises vom 22./23. November 2011, Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/23112011BeschaeftigtenscreeningBegrenzen.html?nn=409242)

Screenings ohne konkreten Tatverdacht nicht zulässig

Folgt man dem Beschluss des Düsseldorfer Kreises, so sind pauschale flächendeckende Datenscreenings ohne konkreten Tatverdacht für die AEO-Zertifizierungen aus Sicht des Datenschutzes nicht zulässig.

9/3 Mitarbeiterscreening zur Terroristenabwehr

Gerade Unternehmen, die internationalen Konzernen angehören, gleichen die Daten ihrer Mitarbeiter gegen sogenannte Antiterrorlisten der EU und der Vereinten Nationen ab.

Auch hier halten die obersten Aufsichtsbehörden, der Düsseldorfer Kreis, in einem Beschluss den Abgleich der Mitarbeiter mit Antiterrorlisten für unzulässig.

§ 28 Abs. 1 BDSG als Erlaubnisnorm nicht zulässig

Der Düsseldorfer Kreis lässt in seiner Argumentation § 28 Abs. 1 BDSG als Erlaubnisnorm für Mitarbeiterscreenings zur Terroristenabwehr nicht zu. Der Abgleich mit den Listen diene nicht dem Vertragsverhältnis. Auch sieht der Düsseldorfer Kreis bei einer Interessenabwägung ein Überwiegen der schutzwürdigen Interessen der betroffenen Mitarbeiter.

(Quelle: Beschluss des Düsseldorfer Kreises vom 23./24. April 2009, Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ DuesseldorferKreis/April09MitarbeiterScreening.html?nn=409242)

Keine rechtliche Verpflichtung zu anlassunabhängigen Screenings

Das Auswärtige Amt hat zum Abgleich von Mitarbeitern mit Antiterrorlisten dem Bundesbeauftragten für Datenschutz mitgeteilt, dass Unternehmen rechtlich nicht zu einem systematischen, anlassunabhängigen Abgleich ihrer Kunden- und Mitarbeiterdaten verpflichtet sind. Eine Pflicht bestehe ausschließlich nach Maßgabe von Sorgfaltspflichten.

(Quelle: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 23. Tätigkeitsbericht 2009/20019, http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23_TB_09_10.html?nn=408924)

Aufgrund der unklaren Lage aus Datenschutzsicht ist auch hier den Unternehmen zu empfehlen, Mitarbeiterscreenings zum Abgleich mit Antiterrorlisten ohne konkreten Tatverdacht auf eine Straftat nicht durchzuführen, außer es würden Sorgfaltspflichten dies gebieten.

Prüfungsfragen zu Mitarbeiterscreenings sind im Tool enthalten.

Toolcheck