Bewerber-Check

Pre-Employment Screening in Zeiten der DSGVO

© privat

Autor
Bernhard Maier
Berufsdetektiv, Buchautor, Inhaber
BM-Investigations

© Viktor Kuryan | Fotolia.com

Stellen Sie sich vor, der neue Datenmanager entpuppt sich als Datendieb, die kürzlich engagierte Niederlassungsleiterin nimmt teure Geschenke an – und der Produktionschef verrät Betriebsgeheimnisse an die Konkurrenz. Korrupte und unloyale Mitarbeiter können Unternehmen erhebliche Schäden zufügen. Pre-Employment Screenings (PES) kann dabei helfen, fehlende Integrität schon vor Vertragsabschluss zu erkennen. Doch welchen Spielraum lässt die europäischen Datenschutzgrundverordnung (EU-DSGVO) den Bewerber-Checks?

Seit Inkrafttreten der DSGVO hat das Bewusstsein um den Schutz personenbezogener Daten stark zugenommen. Kein Wunder. Denn wer gegen den Datenschutz verstößt, muss mit drakonischen Strafen rechnen. Gleichzeitig ist die Verunsicherung in vielen Unternehmen gestiegen. Denn nicht immer ist klar, was in Sachen Datenverarbeitung überhaupt noch erlaubt ist. Das betrifft auch Pre-Employment Screenings. Denn dabei ermitteln und verarbeiten die Beteiligten personenbezogene Daten. Damit berühren sie den Kernbereich der Datenschutzgrundverordnung.

Die zentrale Frage eines Screenings lautet, ob die Einstellung eines bestimmten Bewerbers mit einem Sicherheitsrisiko für den Arbeitgeber verbunden ist. Es geht darum, die Integrität potenzieller Mitarbeiter zu untersuchen. Dafür checken die Prüfer den Lebenslauf des Bewerbers auf Richtigkeit, sammeln Informationen aus öffentlichen Registern oder Datenbanken und holen Auskünfte bei Referenzpersonen ein.

Ist Pre-Employment Screening zulässig?

Personenbezogene Daten zu verarbeiten, ist rechtlich nur zulässig, wenn bestimmte Voraussetzungen erfüllt sind: Wenn die Datenverarbeitung zum Beispiel erforderlich ist, um rechtlichen Verpflichtungen nachzukommen oder berechtigte Interessen zu wahren, dürfen Unternehmen Daten in die Hand nehmen, die sich auf Personen beziehen. Bislang ist noch nicht ausjudiziert, ob im Fall eines Screenings eine der genannten Voraussetzungen gegeben ist. Bei großzügiger Rechtsauslegung könnte sich ein Arbeitgeber auf seine unternehmerische Sorgfaltspflicht (§ 347 UGB) berufen. Auch die arbeitsrechtliche Fürsorgepflicht (§ 1157 ABGB, 18 § AngG) können sie als Argument für ein Screening

samt Datenverarbeitung ins Spiel bringen. Schließlich müssen sie das bestehende Personal vor risikoträchtigen Neuzugängen schützen. Arbeitgeber haben ein berechtigtes Interesse daran, die Daten von Bewerbern zu prüfen. Denn die Pflicht zur Ehrlichkeit bei einer Bewerbung ist keine rechtliche, sondern eine moralische. Daher haben die Bewerber großen Spielraum sich ins rechte Licht zu rücken.

Auch wenn Arbeitgeber die unternehmerische Sorgfalts- und Fürsorgepflicht als Argumente für Pre-Employment-Screening ins Feld führen können, sind sie gut beraten, sich eine schriftliche Einwilligung des Bewerbers geben zu lassen. Dann besteht kein Zweifel an der Zulässigkeit (Art. 6 – EU-DSGVO).

Die DSGVO sieht im Fall der Einwilligungserklärung „Bestimmtheit" vor. Das vom Bewerber unterzeichnete Dokument sollte daher möglichst genau beschreiben, welche Informationen eingeholt werden (zum Beispiel Nachfrage beim Meldeamt, Bonitätscheck, Überprüfen von Diplomen oder Befragung von Referenzpersonen). Führt ein externer Dienstleister das Screening durch, so ist dieser im Dokument anzuführen.

Gelegentlich wird argumentiert, dass die Einwilligung des Bewerbers das Screening ad absurdum führe. Bei einer angekündigten Überprüfung könne der Bewerber zeitgerecht manipulieren, um im schönsten Licht zu glänzen. Doch in der Praxis sind die Möglichkeiten der Manipulation gering. Schnell verändern kann ein Bewerber sein Erscheinungsbild in sozialen Medien. Öffentliche Register (Melderegister, Grundbuch, Firmenbuch, Gewerberegister) und kommerzielle Datenbanken (Bonitätsdienste) entziehen sich seinem Einflussbereich. Referenzpersonen (ehemalige Arbeitgeber, Auskunftspersonen in Bildungseinrichtungen) müssten in einen Täuschungsversuch eingebunden werden, was unwahrscheinlich ist.

Wenn Unternehmen die Überprüfungen offen ankündigen, fördert das zudem die Ehrlichkeit der Bewerber. Denn das Risiko, mit Schönfärberei aufzufliegen, ist den Kandidatinnen und Kandidaten bekannt. Die Einwilligung der Bewerber öffnet zudem Türen, die andernfalls verschlossen blieben. Bildungseinrichtungen bestätigen die Echtheit von Diplomen meist nur dann, wenn eine Einwilligung des Betroffenen vorliegt.

Was tun, wenn Bewerber dem Screening nicht zustimmen?

Die Einwilligung zur Datenverarbeitung kann nur auf freiwilliger Basis erfolgen (Art. 7 – EU-DSGVO). Die Bewerber müssen demnach ihre Einwilligung verweigern dürfen, ohne dadurch einen Nachteil zu erfahren. Mit der Praxis dürfte das teilweise schwer vereinbar sein. Denn meist haben Arbeitgeber einen Grund dafür, dass sie ein Pre-Employment Screening für erforderlich halten. Nehmen wir den Fall eines Arztes, der bei einem Krankenhaus anheuern will, aber dem Überprüfen seiner medizinischen Diplome partout nicht zustimmt. Wäre es aus Sicht des Krankenhauses nicht fahrlässig, die Dokumente ungeprüft zu akzeptieren?

Üblicherweise nimmt mit dem Grad der Qualifikation auch die Verantwortung eines Mitarbeiters und dadurch das Haftungsrisiko des

Arbeitgebers zu. Nachdem der Arbeitgeber für schuldhaftes Fehlverhalten seiner Erfüllungsgehilfen einzustehen hat (§ 1313a ABGB), sind ihm auch Instrumente zur Reduktion des Haftungsrisikos zuzugestehen. Ein solches Instrument stellt PES dar. Verweigert ein hochqualifizierter Bewerber das Screening, kann der Arbeitgeber die Ablehnung mit unkalkulierbarem Haftungsrisiko begründen.

Wann soll gescreent werden?

Da Datenminimierung ein Gebot ist (Art. 5 – EU-DSGVO), sollte das Screening möglichst am Ende eines Recruitingprozesses stattfinden. Somit werden nur Daten von Bewerbern verarbeitet, die ernsthaft für eine Anstellung in Frage kommen. Ein Screening nach Beginn der Beschäftigung ist möglich. Sollte das Ergebnis negativ ausfallen, so können Arbeitgeber das Dienstverhältnis innerhalb einer vereinbarten oder kollektivvertraglichen Probezeit täglich auflösen. Datenschutzrechtlich ist diese Variante optimal, weil nur Daten jener Person verarbeitet werden, die tatsächlich in den Betrieb eingetreten ist. Aus der Sicht des Risikomanagements gilt das eher nicht, denn jeder Tag mit einem riskanten Mitarbeiter ist ein Tag zu viel.

Wie intensiv dürfen Arbeitgeber Bewerber durchleuchten?

Apropos Datenminimierung: Die in der DSGVO verankerte Idee, möglichst wenig persönliche Daten zu bunkern, ist nicht leicht mit Pre-Employment Screening unter einen Hut zu bringen. Im Sinne eines effektiven Risikomanagements ist es natürlich vorteilhaft, möglichst viel über den Bewerber in Erfahrung zu bringen, um ihn gut einschätzen zu können. Die spannende Frage lautet daher, wie intensiv der prospektive Arbeitgeber den Hintergrund eines Bewerbers erforschen darf. Trefflich lässt sich darüber unter Juristen streiten, weil sich dazu bis dato weder Gesetzgebung noch Rechtsprechung einschlägig geäußert haben.

Als genereller Anhaltspunkt zur Frage, wie umfangreich das „Durchleuchten" des Bewerbers ausfallen darf, dient das Risiko jener Position, die zu besetzen ist. Je höher der Schaden ist, den ein Mitarbeiter an der betreffenden Stelle durch Vorsatz oder Unzuverlässigkeit verursachen kann, desto genauer darf die Überprüfung ausfallen. Ein paar gängige Indikatoren für erhöhtes Risiko sind:

- **Nähe zur Geschäftsleitung:** Je näher eine Position im Organigramm bei der Geschäftsleitung angesiedelt ist, umso höher ist in der Regel die Verantwortung dieser Position.
- **Prozesshoheit:** Wenn mit der Position die Hoheit über die Gestaltung von Geschäftsprozessen verbunden ist, so besteht erhöhtes Risiko.
- **Arbeit mit „schwachen" Personengruppen:** Zu den Aufgaben der Position zählt der Umgang mit Kindern, Behinderten oder älteren Menschen.
- **Zugriff auf Geld oder Wertgegenstände:** Es ist besondere Verlässlichkeit erforderlich, weil auf Gelder oder Wertgegenstände des Unternehmens oder von Dritten zugegriffen werden kann.
- **Beaufsichtigung:** Je geringer der Grad der Beaufsichtigung beziehungsweise die Kontrolle des betreffenden Mitarbeiters, desto höher das Risiko.

Als Schaden sind dabei nicht nur finanzielle Verluste zu sehen. Gerade in unfallträchtigem Arbeitsumfeld müssen körperliche Schäden mitbedacht werden, also die Frage, in welchem Ausmaß ein unzuverlässiger Mitarbeiter für Kollegen oder sonstige Dritte zur Gefahr werden kann.

Wie lange dürfen Arbeitgeber die Daten aufbewahren?

Die DSGVO kennt das Prinzip der Zweckbindung (Art. 5 – EU-DSGVO). Daten dürfen Arbeitgeber daher nur für festgelegte und rechtmäßige Zwecke verarbeiten. Daraus leitet sich die Pflicht zur Löschung ab, sobald der Zweck der Verarbeitung wegfällt. Der Zweck des Pre-Employment Screenings besteht darin, Ehrlichkeit, Sicherheit und Zuverlässigkeit des Bewerbers zu überprüfen. Hat sich der prospektive Arbeitgeber dahingehend ein Bild gemacht, so muss er die im Verlauf des Screenings gesammelten Daten löschen.

Bei abgelehnten Bewerbern besteht das Recht zur Datenaufbewahrung für sechs Monate. Es kann nur angeraten werden, von dieser Frist Gebrauch zu machen, da innerhalb dieser Zeit der Bewerber das Arbeitsgericht oder die Gleichbehandlungskommission anrufen und Diskriminierung behaupten kann (§ 15 GIBG, § 29 GIBG). Löscht der Arbeitgeber die Daten vor Ablauf dieser Frist, so könnte er im Beschwerdefall in Beweisnotstand geraten.

Dürfen Arbeitgeber bei den Prüfungen auf soziale Medien zugreifen?

Unter Datenschützern kursiert die Ansicht, man könne soziale Medien in solche mit beruflicher Ausrichtung (LinkedIn, Xing) und solche mit Freizeitorientierung (Facebook, Instagram, Twitter) einteilen. Aufbauend darauf wird die Meinung vertreten, soziale Medien mit Freizeitorientierung seien für den Arbeitgeber tabu.

Es gibt allerdings in Österreich keine juristische Quelle (Gesetz oder gerichtliche Entscheidung), die diese Ansicht stützt. Zudem entspricht die Einteilung anhand der Kriterien Berufs- oder Freizeitorientierung immer weniger der Realität sozialer Medien. Influencer, Blogger und Unternehmen haben Facebook, Instagram und Twitter längst für sich entdeckt und verfolgen dort kommerzielle Interessen.

Darüber hinaus ist es ein Irrtum, dass das Privatleben eines Mitarbeiters den Arbeitgeber nichts angehe. Stellen wir uns einen Lkw-Fahrer vor, der vor Dienstantritt der Brandweinstube seines Vertrauens einen Besuch abstattet und danach „beschwingt" in den Tag starten. Sind seine Promille wirklich Privatsache? Die Faustregel „Privat ist privat" funktioniert nicht. Aktivitäten außerhalb der Arbeitszeit sind dann nicht mehr privat, wenn sie einen Bezug zur Arbeit haben.

Fazit

Datenschutzrechtlich ist in Sachen Pre-Employment Screening leider noch vieles in der Schwebe. Arbeitgeber sollten sich auf das Notwendigste beim Datensammeln beschränken und als Messlatte dafür das Risiko der offenen Position heranziehen. Übermäßiger Datenhunger könnte Pre-Employment Screening ad absurdum führen, weil es als Instrument des Risikomanagements selbst zum rechtlichen Risiko werden kann.