06.06.2024

Bewerberdatenschutz und Recruiting im Fokus

Vor dem Hintergrund der Digitalisierung und des zunehmenden Einsatzes künstlicher Intelligenz (KI) im Bewerbungsprozess ist der Schutz personenbezogener Daten wichtiger denn je. Während die Entwicklung rasant voranschreitet, steigt auch der Beratungsbedarf, weshalb der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) ein besonderes Augenmerk auf den Bewerberdatenschutz als Teilbereich des Datenschutzes legt.

Im Personalbereich ist der Einsatz künstlicher Intelligenz schon seit Jahren etabliert und der massenhafte Einsatz in der Zukunft zu erwarten. Umso wichtiger wird hier der Datenschutz. Vieles ist im Bewerbungsprozess möglich, aber es gibt klare Grenzen, die von Verantwortlichen eingehalten werden müssen. Eine essentielle Grundregel ist, dass Bewerber:innen (für ein Beschäftigungsverhältnis) und Personen, deren Beschäftigungsverhältnis beendet ist, im Datenschutzrecht als Beschäftigte (gemäß § 26 Abs. 8 S. 2 BDSG) gelten und dementsprechend mit Mitarbeiter:innen vergleichbare Datenschutzrechte haben. Ebenso wichtig ist, dass aufgrund der Fragen zur Abgrenzung, wann eine Bewerbung beginnt und wann eine Person als Bewerber:in betrachtet werden kann, Verantwortliche jedes einzelne Stadium des Bewerbungsprozesses gesondert betrachten und rechtlich bewerten müssen.

Bewerbungsunterlagen enthalten eine Vielzahl an sensiblen Daten, die von Namen, Adressen und Geburtsdaten über Ausbildungshistorien und Informationen zu bisherigen Beschäftigungsverhältnissen bis hin zu möglichen Angaben zur Identifikation, Herkunft, Familie und besonderen Kategorien von personenbezogenen Daten wie Gewerkschaftszugehörigkeit, Schwerbehinderungen oder sonstigen Krankheiten reichen. Es ist daher von größter Bedeutung, diese Informationen mit der gleichen Sorgfalt und Diskretion wie bei Mitarbeitenden zu behandeln.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

Um die Privatsphäre von Bewerber:innen zu schützen und die Einhaltung der Datenschutzbestimmungen zu gewährleisten, ist also besondere Sorgfalt geboten.

1. Aktuelle Entwicklungen im Beschäftigtendatenschutz

Am 30. März 2023 hat der Europäische Gerichtshof (EuGH) in der Rechtssache C-34/21 ein Urteil erlassen, das erhebliche Auswirkungen auf die zentrale Rechtsgrundlage des deutschen Beschäftigtendatenschutzes hat. Dieses Urteil wirft Zweifel an der Konformität und damit der Anwendbarkeit des § 26 Abs. 1 Satz 1 BDSG in Bezug auf Datenverarbeitungen im Beschäftigtenkontext auf. Der HmbBfDI hat als erste Aufsichtsbehörde mit einer Pressemitteilung vom 03.04.2023 zu diesem Urteil Stellung genommen und sowohl Unternehmen als auch den Hamburgischen Gesetzgeber dazu aufgefordert, die verwendeten Rechtsgrundlagen erneut zu prüfen. Trotz des Urteils sind Datenverarbeitungsvorgänge im Beschäftigtenkontext nicht ohne Rechtsgrundlage. Gemäß Art. 288 AEUV gilt die DSGVO als EU-Verordnung und somit weiterhin Art. 6 Abs. 1 lit. b DSGVO unmittelbar in allen Mitgliedstaaten als Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung eines Arbeitsvertrages.

Dieses Urteil hat den andauernden politischen Bestrebungen, ein Gesetz zum Beschäftigtendatenschutz zu schaffen, neuen Rückenwind gegeben. Die Datenschutzkonferenz (DSK) hat bereits am 29. April 2022 den Erlass eines solchen bereichsspezifischen Gesetzes in einer Entschließung gefordert. Auch im Koalitionsvertrag Koalitionsvertrag der Bundesregierung ist die Schaffung neuer Regelungen zum Beschäftigtendatenschutz auf Seite 14 bereits benannt. Der dort verankerte Auftrag wird in gemeinsamer Federführung des Bundesministeriums für Arbeit und Soziales (BMAS) und des Bundesministeriums des Innern und für Heimat (BMI) umgesetzt. In einem ersten Schritt haben BMAS und BMI Anfang des Jahres ein gemeinsames Papier mit Vorschlägen der beiden Ressorts zu insgesamt zwölf Regelungsbereichen für ein eigenständiges Gesetz erarbeitet, die sich weitestgehend mit den Forderungen der DSK decken.

2. Grundsätze der DSGVO

Bei der Verarbeitung von Bewerber:innendaten gilt zunächst der Grundsatz der Rechtmäßigkeit und Verarbeitung nach Treu und Glauben (Artikel 5 Abs. 1 lit. a) DSGVO), der Grundsatz der Zweckbindung (gemäß Art. 5 Abs. 1 lit. b) DSGVO) und der Grundsatz der Datenminimierung (gem. Art. 5 Abs. 1 lit. c) DSGVO). Sowohl § 26 BDSG als auch Art. 6 Abs. 1 lit. b DSGVO stellen auf das Kriterium der Erforderlichkeit ab und bestimmen, dass eine Verarbeitung nur dann erfolgen darf, wenn Sie erforderlich ist, um einen Vertrag oder ein Beschäftigungsverhältnis durchzuführen, aufzunehmen oder zu beenden. In diesem Zusammenhang sind auch die Informationspflichten nach Art. 13 und Art. 14 DSGVO zu beachten. In der Praxis des HmbBfDI zeigt sich ein erhöhter Beratungsbedarf hinsichtlich der Informationspflichten, da diese häufig vernachlässigt werden oder Bewerber:innen sich unzureichend oder gar nicht informiert fühlen.

3. Definitionen

Im Bewerbungsverfahren werden zunehmend Anglizismen verwendet. Nicht jedes Unternehmen meint die gleichen Verarbeitungsvorgänge, wenn Begriffe wie Recruiting, Open-Sourcing, Talent-Management oder AI verwendet werden. Auch wenn es keine einheitlichen Definitionen für diese Begriffe gibt, ist es ratsam, sich auf einen einheitlichen Sprachgebrauch zu einigen und im Zweifelsfall immer nachzufragen oder zu informieren, welche Verarbeitungen stattfinden. Der HmbBfDI versteht die nachfolgenden Begriffe wie folgt:

Recruiting bezeichnet eine Personalbeschaffung oder Personalvermittlung, umfasst alle Aktivitäten, die darauf abzielen vakante Stellen zu besetzen. Mitumfasst sind Stellenanzeigen, Veröffentlichungen, Vorstellungsgespräche, Vertragsunterzeichnungen und Onboarding-Prozesse.

Headhunter/Talentscouts: Headhunting bezeichnet die Suche nach Fach- und Führungskräften auf Erfolgsbasis, oftmals im Auftragsverhältnis und insbesondere unter Nutzung von Sozialen Medien und Business-Plattformen.

Active Sourcing bezeichnet eine aktive Personalbeschaffung, also Maßnahmen eines Unternehmens, um proaktiv potenzielle Bewerber:innen zu identifizieren. Erreicht werden sollen insbesondere auch Kandidat:innen, die nicht aktiv nach einem Job suchen.

Background-Checks/Pre-Employment-Checks sind auch bekannt als Bewerber:innen-Screening/Überprüfung von Kandidat:innen. Es handelt sich um Überprüfungen, die

Arbeitgeber:innen durchführen, um die Angaben und Hintergründe der Kandidat:innen vor der Einstellung zu verifizieren, bei Dritten oder über Internetrecherchen. Nicht umfasst sind Sicherheitsüberprüfungen der Mitarbeiter:innen nach einschlägigen Sicherheitsüberprüfungsgesetzen (z.B.zum Beispiel SÜG und LuftSiG).

Ein **Talentpool** ist eine Datenbank oder Online-Plattform, die Profile von Bewerber:innen, Mitarbeiter:innen, Freiberufler:innen oder anderen externen Kontakten enthält, welche für eine Stellenbesetzung in Betracht kommen.

Die Begriffe **CV Parsing/Resume Parsing** bezeichnen das automatisierte Auslesen von Bewerbungen (insbesondere Anschreiben und Lebenslauf). Die ausgelesenen Daten werden sodann ebenfalls automatisch in ein Bewerbungsmanagementsystem (BMS) überführt.

4. Phasen im Recruiting-Prozess

Der Rekrutierungsprozess lässt sich im Wesentlichen in verschiedene Phasen unterteilen, die von der Erstansprache potenzieller Kandidat:innen (Kaltakquise) bis hin zur Entscheidung für (Auswahl) oder gegen (Ablehnung) einzelne Bewerber:innen reichen.
In jeder Phase finden unterschiedliche Aktivitäten statt, die von einem oder mehreren Beteiligten durchgeführt werden und verschiedene rechtliche Beziehungen betreffen. So wird eine Person, die sich die Karriereseite lediglich ansieht, zu einer aktiven Bewerber:in, wenn sie ihre Informationen in das Bewerbungsformular eingibt. Sofern für Verarbeitungen der § 26 Abs. 1 S. 1 BDSG keine Anwendung mehr findet (siehe oben), ist eine Abgrenzung über das Erforderlichkeitskriterium des Art. 6 Abs. 1 lit. b DSGVO vorzunehmen, unabhängig davon, ob es sich bereits um eine Bewerber:in handelt oder nicht.
Um eine bessere Übersicht zu gewährleisten und den Anforderungen des Art. 30 Abs. 1 DSGVO gerecht zu werden, ist es sinnvoll, einen Überblick über alle Phasen des Bewerbungsverfahrens sowie die dazugehörigen Verarbeitungsvorgängen zu erstellen. Eine trennscharfe Abgrenzung der einzelnen Phasen muss dabei nicht vorgenommen werden. Möglich ist es selbstverständlich auch, dass einzelne Verarbeitungssituationen in verschiedenen Phasen vorkommen. Die Übersicht ist insofern nicht als abschließende Aufzählung zu verstehen. Eine solche Übersicht könnte beispielhaft wie in Abbildung 1 aussehen und die Verantwortlichen dabei unterstützen, die Verarbeitungsvorgänge auf die korrekten Rechtsgrundlagen zu stützen.

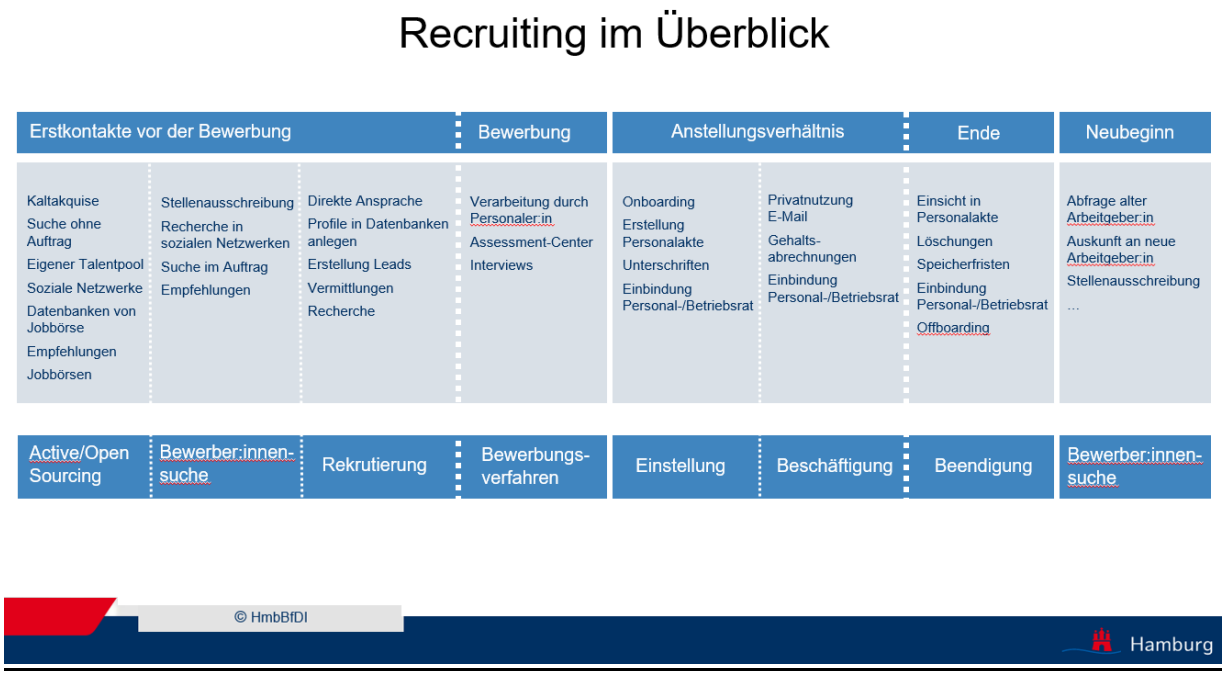

Abbildung 1: Phasen im Recruiting-Prozess

5. Talentpools – Aufnahme nur mit Einwilligung

Die Aufnahme in sogenannte Talentpools ist grundsätzlich möglich, vorausgesetzt, die Bewerber:innen erteilen eine ausdrückliche Einwilligung. Es ist wichtig, dass diese Einwilligung unter Beachtung der Informationspflichten gemäß Art. 13 DSGVO vollständig transparent und freiwillig erteilt wird. Die Einwilligung sollte in Textform erfolgen und mindestens die folgenden Inhalte enthalten:

- Zweck der Datenspeicherung im Talentpool
- welche Daten werden verarbeitet
- Dauer der Speicherung
- Möglichkeit zum Widerruf der Einwilligung
- Information gem. Art. 13 DSGVO
- gegebenenfalls Information gemäß Art. 14 DSGVO

Die Informationen gemäß Art. 13 DSGVO können in die Einwilligungserklärung integriert werden. In der Praxis ergeben sich oft Herausforderungen im Bereich der Speicherdauer dieser Daten, insbesondere bei der Etablierung einer angemessenen Löschfrist. Es ist wichtig zu beachten, dass Einwilligungen nicht unbegrenzt gültig sind. In der Praxis kommt es vor, dass zwar eine Einwilligung eingeholt, jedoch kein Zeitraum für die Speicherdauer festgelegt wird. In den allermeisten Fällen hat dies zur Folge, dass die Daten unbegrenzt gespeichert werden. Zu empfehlen ist daher, die Einwilligung zunächst für einen angemessenen Zeitraum einzuholen und nach Ablauf dieses Zeitraums erneut um Einwilligung zu bitten. Reagieren die betroffenen

Personen nicht, müssen die Daten unverzüglich und unwiederbringlich gelöscht werden. Abhängig von den branchenüblichen Anforderungen an die Stellen kann es zu unterschiedlichen Löschfristen kommen. Daher sind Speicherfristen von einigen Monaten bis hin zu mehreren Jahren in Einzelfällen denkbar. Diese hängen davon ab, wie lange es üblicherweise dauern würde, eine entsprechende Stelle zu besetzen, und sind mit möglichen Klagefristen und Ausnahmeregelungen gemäß Art. 17 Abs. 3 DSGVO verbunden.

6. Background-Checks orientieren sich am Fragerecht im Bewerbungsgespräch

In der Regel können Informationen über die Bewerber:in bei ihnen direkt eingeholt werden. Das nachvollziehbare Bedürfnis, weitere Informationen über sie zu erlangen, muss in datenschutzrechtlichen Grenzen erfolgen. Die herkömmlichen Methoden Bewerber:innen kennenzulernen, wie zum Beispiel Bewerbungsgespräche, Assessment-Center, Qualifikationen oder Arbeitszeugnisse, sollten hierfür ausreichen. Auch wenn eine Internetrecherche über Suchmaschinen oder die Suchfunktion sozialer Netzwerke Suche nicht per se ausgeschlossen ist, müssen Verantwortliche die unterschiedlichen Netzwerke voneinander differenzieren. Sofern Informationen bei Dritten eingeholten werden, sind ebenfalls die Informationspflichten gem. Art. 14 DSGVO zu beachten.

Nicht alle Informationen dürfen berücksichtigt werden

Informationen, die über das Fragerecht im Bewerbungsgespräch hinausgehen, müssen unter Umständen unberücksichtigt bleiben (zum Beispiel Schwangerschaft, Gesundheitsdaten, politische Zugehörigkeit, Google-Überschriften). Das gilt auch bei Informationen, die zufällig erlangt oder auf andere Weise bekannt geworden sind. Innerhalb dieser Bereiche sollten Bewerber:innen aufgrund der schwierigen Beweislage selbst darauf achten, ein angemessenes Bild von sich in den sozialen Medien zu präsentieren. In der Praxis wird es sich oftmals nicht vermeiden lassen, dass ein „Zufallsfund“, der gegebenenfalls datenschutzrechtlich unzulässig wäre, sich zu Ungunsten der Bewerber:in auswirkt, ohne dass die betroffene Bewerber:in jemals über diesen Umstand informiert würde.

Internetrecherche – die Zielrichtung der Informationspreisgabe entscheidet über die Verwertbarkeit

Sollten soziale Netzwerke und Suchmaschinen herangezogen werden, muss zwischen beruflichen und privaten Netzwerken unterschieden werden, ebenso wie hinsichtlich des Zwecks der Informationspreisgabe. Private Netzwerke dürfen nicht für Background-Checks herangezogen

werden. Zu berücksichtigen ist ferner, dass auch in beruflichen Netzwerken die Möglichkeit besteht, private Informationen preiszugeben. Ein bekanntes Beispiel für ein überwiegend privates Netzwerke ist Facebook, während LinkedIn hauptsächlich beruflich genutzt wird. Der Wandel dieser Plattformen und die damit verbundene Unterscheidung nach dem Zweck der Informationsfreigabe zeigt sich jedoch an Plattformen wie X (ehemals Twitter), das sowohl für berufliche als auch für private Zwecke genutzt wird.

7. KI-Anwendungen

Von der Veröffentlichung einer Stellenausschreibung über die automatisierte Vorauswahl von Bewerber:innen bis hin zur Analyse von Bewerbungsgesprächen und dem Einsatz von Chatbots bieten KI-Systeme Erleichterungen und Automatisierungsmöglichkeiten im Bewerbungsprozess. Mit den zur Verfügung stehenden Technologien sind datenschutzrechtliche Herausforderungen verbunden. Der HmbBfDI erhält regelmäßig Anfragen zu verschiedenen Softwarelösungen, darunter Lebenslaufparser und Emotionsanalysen. Im Hinblick auf den Einsatz von LLM Chatbots hat der HmbBfDI am 13. November 2023 eine Checkliste veröffentlicht. Diese soll Unternehmen und Behörden als Leitfaden für den datenschutzkonformen Einsatz von Chatbots dienen. Darüber hinaus hat die DSK am 6. Mai 2024 eine Orientierungshilfe für den Einsatz von KI-Programmen veröffentlicht. Diese Orientierungshilfe soll einen Überblick über die datenschutzrechtlichen Kriterien bieten, die bei der datenschutzkonformen Nutzung von KI-Anwendungen zu berücksichtigen sind. Sie dient als Leitfaden für die Auswahl, Implementierung und Nutzung von KI-Anwendungen.

Lebenslaufparser – entscheidend sind die Verarbeitungsmöglichkeiten

Der Einsatz ist grundsätzlich zulässig, wenn personenbezogene Daten ausgelesen und strukturiert in ein Bewerbungsmanagementsystem (BMS) übertragen werden. Dabei muss der Grundsatz der Datenrichtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO beachtet werden. Sollte nach dem Parsing eine zusätzliche Datenanalyse durchgeführt werden, muss Art. 22 DSGVO eingehalten werden, der sich mit automatisierten Einzelfallentscheidungen befasst. Zudem ist das Urteil des Europäischen Gerichtshofs (EuGH) zur Schufa vom 07.12.2023 zu berücksichtigen. Gemäß Art. 22 Abs. 1 DSGVO und dem EuGH-Urteil dürfen Entscheidungen mit Rechtswirkung grundsätzlich nur von Menschen getroffen werden. KI-Vorschläge, die Rechtswirkungen für Betroffene haben, müssen so gestaltet sein, dass die entscheidende Person einen echten Entscheidungsspielraum hat und nicht hauptsächlich auf Grundlage des KI-Vorschlags entscheidet. Eine bloß formelle menschliche Beteiligung ist nicht ausreichend.

Emotionsanalysen – grundsätzlich unzulässig

Emotionsanalysen im Bewerbungsverfahren bezeichnen den Einsatz von Technologien, die die emotionalen Zustände und Reaktionen von Bewerber:innen während des Bewerbungsprozesses erkennen und interpretieren sollen. Diese Analyse kann durch verschiedene Methoden erfolgen, darunter Mimik- und Gestikanalyse, Sprach- und Tonfallanalyse oder die Auswertung von schriftlichen Antworten. Das Ziel ist, Rückschlüsse auf die Persönlichkeit, Motivation und potenzielle Eignung der Bewerber:in zu ziehen.
Im Bewerbungsverfahren sind Emotionsanalysen datenschutzrechtlich problematisch, weil sie in der Regel nicht erforderlich sind und die Freiwilligkeit der Einwilligung zweifelhaft sein könnte. Ebenfalls muss geprüft werden, ob es sich um die Verarbeitung von biometrischen Daten handelt (vergleiche hierzu auch das DSK-Positionspapier zur biometrischen Analyse vom 03. April 2019). Insoweit besteht ein Gleichlauf mit der KI-Verordnung, welche gemäß Art. 5 Abs. 1 lit. f KI-VO die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz (mit wenigen Ausnahmen wie medizinischen Aspekten oder Sicherheitsaspekten) als verbotene Praktik aufführt.

LLM-Chatbots – sinnvoll für Stellenausschreibungen

KI-basierte Systeme wie Large Language Models (LLM) und Chatbots können im Bewerbungsprozess vielfältige Aufgaben übernehmen, beispielsweise die Formulierung von Einladungen oder Absagen, die Beantwortung häufig gestellter Fragen, die Durchführung von ersten Auswahlgesprächen oder die Bereitstellung von Informationen über den Bewerbungsablauf. Häufig stellt die datenschutzkonforme Integration solcher LLM-Chatbots die Verantwortlichen vor datenschutzrechtliche Herausforderungen.
Eine vollständige Auswahlentscheidung oder einen finalen Kandidatenvorschlag dem LLM-System zu überlassen, ist aus datenschutzrechtlicher Sicht problematisch und grundsätzlich unzulässig. Solche automatisierten Entscheidungen müssen den Anforderungen des Artikels 22 der Datenschutz-Grundverordnung (DSGVO) genügen.

8. Ausblick

Der Einsatz von Künstlicher Intelligenz (KI) im Recruiting wird in Zukunft weiter an Bedeutung gewinnen. Gleichzeitig steigen auch die datenschutzrechtlichen Anforderungen. Neben der Datenschutz-Grundverordnung (DSGVO) werden neue Regulierungen wie das KI-Gesetz beziehungsweise die KI-Verordnung der Europäischen Union eine wichtige Rolle spielen.

Unternehmen sind dazu angehalten, strenge Datenschutzrichtlinien einzuhalten und transparente Verfahren zu implementieren.
Die Integration datenschutzkonformer automatisierter Analysen kann unter Umständen den gesamten Recruiting-Prozess auch positiv beeinflussen, indem sie personalisierte, faire und diskriminierungsfreie Bewerbungsverfahren ermöglicht. Dabei wird die Herausforderung darin bestehen, eine Balance zwischen technologischen Fortschritten und dem Datenschutz der Bewerber:in zu finden. Verantwortliche sollten sich proaktiv mit den Anforderungen auseinandersetzen und entsprechende Einsatzmöglichkeiten datenschutzkonform umsetzen, um damit rechtliche Risiken zu minimieren und das Vertrauen potenzieller Mitarbeiter:innen und Bewerber:innen zu gewinnen und die eigene Außenwirkung zu stärken.

Kontakt für Rückfragen:

Eva Zimmermann
Telefon: +49 40 428 54-4044
E-Mail: presse@datenschutz.hamburg.de