Zum Thema

Über die Autorinnen

Mag. Judith Leschanz leitet den Bereich Data Privacy bei A1, verantwortet die strategische Ausrichtung des Data Privacy Managements und agiert als Vorsitzende des Datenschutzbeirats. Sie hat langjährige Erfahrung in unterschiedlichen Managementpositionen bei der Telekom Austria Group im In- und Ausland. Zusätzlich ist sie Vorstandsvorsitzende des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at tätig. E-Mail: judith.leschanz@A1telekom.at

Mag. Sabine Gölles, MA, ist Juristin im Bereich Data Privacy bei A1 und absolvierte zusätzlich den Masterstudiengang „ IT-Recht & Management" der FH Joanneum in Kapfenberg. E-Mail: sabine.goelles@a1telekom.at

Karin Tien
Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte OG

Online-Bewerbungsverfahren: Umgang mit Bewerberdaten zur Begründung eines Beschäftigungsverhältnisses

Was müssen Arbeitgeber bei der Suche nach neuen Talenten beachten? Zur Vereinfachung und Optimierung des Bewerbungsprozesses setzen Unternehmen weiterhin vermehrt elektronische Bewerbungsplattformen ein. Einerseits um den Rekrutierungsvorgang mittels Bewerberportal und vorgegebener Eingabemasken zu beschleunigen, andererseits um das Bewerbermanagement zu vereinheitlichen.

Informationsinteresse des Arbeitgebers vor Begründung eines Beschäftigtenverhältnisses

Elektronische Bewerbungsplattformen ersetzen zunehmend die klassische Bewerbung per Post oder E-Mail. Eigens eingerichtete Onlineportale forcieren das Anlegen eines Bewerberprofils und kategorisieren in Form von Eingabefeldern (wie Ausbildungsabschlüsse oder Sprachkenntnisse) geeignete Kandidaten. Solche Plattformen bieten oft die Möglichkeit an, Dokumente hochzuladen und dem Unternehmen zur Verfügung zu stellen. Für Bewerber, die sich in der „Job-Warteschleife" befinden, ist eine zeitlich nachgelagerte Bearbeitung der Daten in manchen Fällen ebenfalls vorgesehen. So können Bewerber – je nach Ausgestaltung des Bewerbungsportals – zu einem späteren Zeitpunkt entweder wieder in das Bewerberportal einsteigen und ihre Angaben anpassen oder aber das Profil endgültig löschen.

Im Gegensatz zur Zusendung der Daten durch den Bewerber per E-Mail werden die über ein Bewerberportal erhaltenen Informationen **direkt in einer Datenbank gespeichert**. Daten interessanter Kandidaten erfüllen für Unternehmen zudem den weiteren Zweck, einen Datenpool für zukünftige Stellenbesetzungen aufzubauen.

Prinzipiell wird zwischen firmeneigenen Bewerberplattformen, also der Nutzung des Portals ausschließlich durch ein Unternehmen, und dem Einsatz von Bewerbermanagement-Softwaresystemen unterschieden, die von externen Anbietern betrieben werden. Neben diesen beiden Lösungen finden sich **auch Social-Media-Plattformen**, die ebenfalls Unterstützung bei der Personalbeschaffung anbieten (wie Xing, LinkedIn). Der markanteste Unterschied aller E-Recruiting-Plattformen zur klassischen E-Mail-Bewerbung ist neben der datenschutzrechtlichen Implikation, dass die Strukturierung der Daten durch die Eingabefelder nicht vom Bewerber selbst abhängt.[1]

Mit den Daten der Kandidaten bauen Unternehmen einen Pool für Stellenbesetzungen auf.

Art 88 Abs 1 DSGVO erlaubt es Mitgliedstaaten, *„spezifischere Vorschriften"* zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigungsdaten im Beschäftigungskontext zu erlassen.[2] Neben den in § 29 DSG (neu) geregelten arbeitsverfassungsrechtlichen Bestimmungen zu den bisherigen Mitwirkungsrechten und Befugnissen des Betriebsrats[3] werden im Anwendungsbereich der **DSGVO Bewerberdaten** im Sinne des Beschäftigtendatenschutzes ebenfalls **mitumfasst**.[4]

Erhebung, Verarbeitung und Nutzung von Bewerberdaten

Das Informationsinteresse des Arbeitgebers erfordert vor der Begründung des Beschäftigungsverhältnisses keine Angaben, die während einem aufrechten Arbeitsverhältnis benötigt werden.[5] Demzufolge sind bei der Erhebung der Daten mittels Eingabemaske einer Bewerberplattform Erkundigungen über den Familienstand, Angaben zur Pflichtversicherung oder religiöse Ansichten für die Einstellungsentscheidung in der Regel irrelevant und sollten während eines Bewerbungsverfahrens nicht anzugeben sein. Diese Informationen gewinnen möglicherweise erst ab Eintritt in ein Beschäftigungsverhältnis an Bedeutung und sind folglich erst im Zuge einer tatsächlichen Einstellung zu erheben.

Das kürzlich veröffentlichte Arbeitspapier der Art-29-Datenschutzgruppe setzt

[1] Vgl Broy in *Weth/Herberger/Wächter* (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014) Personenbezogene Daten im Internet Rz 69. [2] VO (EU) 679/2016 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1. [3] 332/ME 25. GP 15. [4] „Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung" iSd Art 88 Abs 1 DSGVO 679/2016, ABl L 2016/119, 1. [5] Vgl *Gola/Pötters/Wonka*, Handbuch Arbeitnehmerdatenschutz[7] (2016) Rz 619.

sich ebenfalls mit dem Beschäftigtendatenschutz hinsichtlich der Bewerberdaten auseinander.[6] Basierend auf den darin festgehaltenen Empfehlungen der Art-29-Datenschutzgruppe müssen Bewerber jedenfalls darüber informiert werden, welche Daten im Laufe des Bewerbungsverfahrens (auch bei späterem „Online Assessment Center") verarbeitet werden, noch bevor diese die Bewerberplattform nutzen.

Die **Einwilligung des Bewerbers** ist somit vor Eingabe der Bewerberdaten einzuholen und das Unternehmen hat dabei sicherzustellen, dass

- der Nutzer des Bewerbungsportals diese Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung nachweisbar ist und protokolliert wurde und
- der Nutzer den Inhalt der abgegebenen Einwilligung jederzeit widerrufen kann.

HINWEIS/PRAXISTIPP

Ein einfacher Hinweis auf die Datenschutzerklärung oder ein Link hierauf ist unzureichend: Laut der Art-29-Datenschutzgruppe soll zumindest ein aktives Element (Checkbox-Lösung) bei der Einholung der Zustimmung des Bewerbers erforderlich sein.

In diesem Zusammenhang ist jedoch zu betonen, dass der nach Art 6 Abs 1 lit a DSGVO bestehende Erlaubnistatbestand der Einwilligung im Bereich des Beschäftigtendatenschutzes kritisch zu beurteilen ist,[7] da ein „In-Verbindung-setzen" der Einholung der Einwilligung mit einem in Aussicht gestellten (Arbeits-)Vertrag dem **Kopplungsverbot** iSd Art 7 Abs 4 DSGVO (Abhängigkeitsverhältnis) entgegenstehen dürfte.[8]

Weitergabe der Bewerberdaten im Konzern

Gerade Konzerngesellschaften setzen Online-Bewerbungsplattformen vorrangig ein, um damit Ressourcen der Personalbeschaffung und -planung zu bündeln. Neben der Informationspflicht über die Verwendung der Bewerberdaten, die gegenüber den Bewerbern einzuhalten ist, wird für die Datenweitergabe im Konzern, sofern mehrere Konzernunternehmen die Bewerbungsdaten erhalten sollen, oder Zugriff auf diese haben werden die Einholung der Einwilligung zur Verwendung der Daten durch eine Unternehmensgruppe notwendig sein.

HINWEIS/PRAXISTIPP

Die Zustimmungserklärung sollte die teilnehmenden Unternehmen anführen, die die Bewerberdaten ebenfalls erhalten.

Speicherdauer von Bewerberdaten

Neben einer Ausweitung der bewährten Betroffenenrechte, insb bei den Informationspflichten und Auskunftsrechten, enthält die DSGVO neue Rechte, die wesentlich für den Beschäftigtendatenschutz sind. Ein besonders wichtiger Anspruch ist hinsichtlich der Speicherung von Informationen über Bewerber das **„Recht auf Vergessenwerden"** (Art 17 DSGVO).

Ohne Zustimmung der Bewerber zur Verwendung und weiteren Speicherung ihrer Bewerbungsdaten dürfen die Daten nur so lange aufbewahrt werden, wie dies gesetzlich zulässig und gerechtfertigt ist. Es existiert keine eigene gesetzliche Grundlage, die die Speicherdauer von Bewerberdaten konkret regelt. Nach allgemeinen Grundsätzen dürfen Bewerberdaten daher nur so lange aufbewahrt werden, wie das Bewerbungsverfahren andauert, eine Initiativbewerbung nicht in Betracht gezogen wird oder der Bewerber mögliche Ansprüche geltend machen kann.

Eine längere Speicherung von Bewerberdaten benötigt die Zustimmung der Kandidaten.

Ansprüche von Bewerbern können sich beispielsweise auf das Gleichbehandlungsgesetz (wie eine behauptete Diskriminierung abgelehnter Bewerber, §§ 15, 29 GlBG) oder § 7e iVm § 7k Abs 2 Z 1 BEinstG stützen. Diese Ansprüche können bis zu sechs Monate nach Beendigung des Bewerbungsverfahrens geltend gemacht werden. Folglich dürfen Bewerberdaten ohne Zustimmung der Bewerber maximal bis zu **sechs Monate** lang aufbewahrt werden.[9]

Daten, die während des Bewerbungsprozesses verarbeitet worden sind, sollten in der Regel gelöscht werden, sobald deutlich wird, dass es nicht zur Besetzung der vakanten Stelle kommt, da entweder das Bewerbungsverfahren beendet ist oder ersichtlich wird, dass das Beschäftigungsangebot vom Bewerber ausgeschlagen wird. Eine längere Evidenzhaltung in der Bewerberdatenbank benötigt die Zustimmung der Kandidaten.

Profiling und Bewerbermanagement-Tools

Problematisch kann bei Einsatz einer Online-Bewerbungsplattform die Auswahl der Bewerber hinsichtlich des Grads einer automatisierten Entscheidung sein. Eine ausschließlich auf eine automatisierte verarbeitungsgestützte Entscheidung könnte als „Profiling" gem Art 22 DSGVO datenschutzrechtlich unzulässig sein.[10]

Dabei kommt es nicht darauf an, ob der gesamte Entscheidungsprozess bei der Bewerberauswahl nur durch das Programm (Algorithmus) bestimmt und in letzter Entscheidungsinstanz von der zuständigen natürlichen Person formell bestätigt wird.[11] Ausschlaggebend ist es inwieweit eine natürliche Person Einfluss auf die Entscheidungsfindung hat, weshalb es ratsam ist, die inhaltliche Mitverantwortung der Entscheidungsfindung durch einen Mitarbeiter der Personalabteilung begleiten zu lassen und ein mögliches Abweichen von der automatisierten Entscheidungsfindung gegebenenfalls zuzulassen.[12]

Zusammenfassung und Ausblick

Die Zukunft der Personalbeschaffung hat schon längst Ausschreibungen im Internet für sich entdeckt und den Wirkungskreis auf der Suche nach „High Potentials" durch crossmediale Kampagnen erweitert. Ziel ist es, unverfänglich und rasch mit potentiellen Bewerbern Kontakt aufzunehmen oder in einen Dialog zu treten. Ob Einstellungsgespräch über Skype, Entgegennahme von Bewerbungsvideos via Snapchat oder Einsatz von Recruiting Robots, alle diese neuen Bewerbungstrends lassen erahnen, welche datenschutzrechtlichen Problemstellungen sich beim Einsatz von zukünftigen E-Recruiting-Strategien noch ergeben könnten.

Die DSGVO und das DSG (neu) stellen die wesentlichen Grundlagen für die Verarbeitung von Beschäftigtendaten dar und gewinnen, neben der Stärkung der Betroffenenrechte, auch wegen des strikteren Sanktionsmechanismus an Bedeutung. Bereits bestehende Bewerberportale sollten nun

[6] Art-29-Datenschutzgruppe, Opinion 2/2017 on data processing at work (WP 249) 11. [7] Vgl *Kort*, Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung (DS-GVO), NZA-Beilage 2016, 65. [8] Siehe auch *Gorcnik*, Die Einwilligung des Arbeitnehmers als Rechtsgrundlage einer Datenverarbeitung nach der DSGVO, Dako 2017/33, sowie die Entscheidungsbesprechung zu DSB 22. 5. 2017, DSB-D216.396/0003-DSB/2017, von *Haidinger* in diesem Heft Seite 92. [9] Siehe dazu *Gorcnik*, Datenschutz im Bewerbungsverfahren, ecolex 2013, 57. [10] Vgl *Kort*, Eignungsdiagnose, NZA-Beilage 2016, 71. [11] *Suda* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Kommentar zur Datenschutz-Grundverordnung (2017) 242. [12] *Buchner* in *Kühling/Buchner* (Hrsg), DS-GVO Datenschutzgrundverordnung (2017), Automatisierte Entscheidungen im Einzelfall einschließlich Profiling Rz 15.

auf die Erfüllung der Anforderungen im Kontext der DSGVO, wie der Wahrung der Betroffenenrechte und Einholung der Zustimmung, überprüft und gegebenenfalls nachjustiert werden.

Dako 2017/55

Zum Thema

Über die Autorin

Mag. Karin Tien ist Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte OG und auf Datenschutz-, IT- und Telekommunikationsrecht spezialisiert. E-Mail: tk@kt.at

Literatur

Kort, Eignungsdiagnose von Bewerbern unter der Datenschutz-Grundverordnung (DS-GVO), NZA-Beilage 2016, 62; *Weth/Herberger/Wächter* (Hrsg), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis (2014); *Gola/Pötters/Wonka*, Handbuch Arbeitnehmerdatenschutz[7] (2016); *Gerhartl*, Datenschutz im Bewerbungsverfahren, ecolex 2013, 57; *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Kommentar zur Datenschutz-Grundverordnung (2017); *Kühling/Buchner* (Hrsg), DS-GVO Datenschutzgrundverordnung (2017).

Hans-Jürgen Pollirer
Geschäftsführer der Secur-Data Betriebsberatungs-GmbH

Checkliste für die Einwilligungserklärungen der Art 7 und 8 DSGVO

Altersgrenze; Freiwilligkeit; Widerruf; Transparenzgebot. Angesichts der in Art 83 Abs 4 lit a und Abs 5 lit a DSGVO bei einem Verstoß gegen die Bestimmungen der in Art 7 und 8 DSGVO vorgesehenen Geldbußen sollte dem Thema „Einwilligung" seitens der Verantwortlichen ein hoher Stellenwert eingeräumt werden. Die nachfolgende Checkliste soll Sie bei der Überprüfung bzw Überarbeitung Ihrer derzeit in Verwendung stehenden Einwilligungserklärungen unterstützen.

Rechtliche Grundlagen

Wie Art 7 RL 95/46/EG und § 7 iVm §§ 8 und 9 DSG 2000 verbietet auch die DSGVO jede Verarbeitung personenbezogener Daten, soweit nicht ein entsprechender Ausnahmetatbestand vorliegt, der die Verarbeitung legitimiert. Hierbei kommt gerade der „Einwilligung" (nach § 4 Z 14 DSG 2000 als „Zustimmung" bezeichnet) der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten im Datenschutzrecht – als Ausdruck ihres informationellen Selbstbestimmungsrechts – eine wichtige Schlüsselrolle zu.

Die Definition der Einwilligung des **Art 4 Z 11 DSGVO** enthält im Vergleich zu den Definitionen des Art 2 lit h RL 95/46/EG und § 4 Z 14 DSG 2000 keine besonderen Unterschiede. Wie auch nach der derzeitigen Rechtslage muss eine wirksame Einwilligung ohne Zwang und in Kenntnis für den konkreten Fall abgegeben werden.

Art 7 iVm ErwGr **32, 33, 42 und 43 DSGVO** enthält die „Bedingungen für die Einwilligung". Grundsätzlich sollte man eine Einwilligung des Betroffenen erst dann einholen, wenn für die Verarbeitung keine andere Rechtsgrundlage – zB die Verarbeitung ist für die Erfüllung eines Vertrags notwendig – vorliegt, da die betroffene Person nach den Bestimmungen des Art 7 Abs 3 DSGVO das Recht hat, ihre Einwilligung jederzeit zu widerrufen.

PRAXISTIPP

Die in der Praxis häufige Vorgehensweise, trotz Vorhandensein einer anderen Rechtsgrundlage zusätzlich eine Einwilligung der betroffenen Person – quasi aus Sicherheitsgründen – einzuholen, sollte vermieden werden, weil dies keine zusätzliche Legitimierung ergibt.

Art 8 iVm ErwGr 38 DSGVO enthält erstmals im europäischen Datenschutzrecht eine ausdrückliche gesetzliche Regelung in Bezug auf die Einwilligung von **Kindern und Jugendlichen**, allerdings gelten diese Bestimmungen nur eingeschränkt bei einem Angebot von Diensten der Informationsgesellschaft (zB Angebote eines Webshops). Art 8 Abs 1 DSGVO setzt zwar die Altersgrenze für die Zustimmungsfähigkeit mit der Vollendung des 16. Lebensjahrs fest, eröffnet aber den MS die Möglichkeit, eine niedrigere Altersgrenze vorzusehen. Während im Entwurf des am 12. 5. 2017 veröffentlichten Datenschutz-Anpassungsgesetzes die Altersgrenze noch mit 16 Jahren festgelegt wurde, wurde diese – offensichtlich auf Intervention der Wirtschaft – im am 29. 6. 2017 im Nationalrat beschlossenen Datenschutz-Anpassungsgesetz auf 14 Jahre abgesenkt. Unter dieser Altersgrenze ist eine Zustimmungserklärung von Kindern nur mit Einwilligung der Obsorgeberechtigten (va Eltern) gültig.

Voraussetzungen Einwilligung

Kurz zusammengefasst muss eine rechtsgültige Einwilligungserklärung folgende **Voraussetzungen** erfüllen:

- Nachweisbarkeit der erteilten Einwilligung durch den Verantwortlichen;
- das Ersuchen um Einwilligung muss in leicht verständlicher und leicht zugäng-