Checkliste: Datenschutz

Datensicherheit im Bewerbermanagement

Während des gesamten Recruiting-Prozesses sammeln sich zahlreiche personenbezogene und schützenswerte Informationen von Bewerbern im Unternehmen an. Insbesondere bei der Nutzung eines cloudbasierten Bewerbermanagementsystems gibt es einige wichtige Fragen, die Sie klären sollten, um sicherzustellen, dass Ihre Recruiting-Software Sie beim Thema Datenschutz nicht im Stich lässt!

Datenschutz und Datensicherheit - worum geht es?

Beim Begriff „Datenschutz“ geht es um den Schutz der Privatsphäre eines jeden Menschen. Datenschutz garantiert jedem Bürger ein Recht auf informationelle Selbstbestimmung und schützt ihn vor missbräuchlicher Verwendung seiner Daten. Für die Verarbeitung personenbezogener Daten gibt es Regeln, die hauptsächlich im Bundesdatenschutzgesetz bzw. den Datenschutzgesetzen der Länder niedergelegt sind. Hier wird also danach gefragt, ob personenbezogene Daten überhaupt verarbeitet werden dürfen.

„Datensicherheit“ befasst sich generell mit dem Schutz von Daten, unabhängig davon, ob diese personenbezogen sind oder nicht. Daten sollen vor Manipulation, Verlust oder unberechtigter Kenntnisnahme geschützt werden. Hier geht es also um die Frage, welche Maßnahmen ergriffen werden müssen, um Daten optimal zu schützen. Die Datensicherheit muss durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen sichergestellt werden, bspw. durch Passwortschutz, Zutrittskontrollen, etc.

Datenschutz und Datensicherheit im Recruiting

Bei der Verwaltung und Bearbeitung von Bewerberdaten fallen viele personenbezogene Daten an, die selbstverständlich dem Datenschutz unterliegen müssen.
Sobald ein Unternehmen ein Bewerbermanagement-System zur Administration der Bewerberdaten verwendet, ist die Software elementarer Bestandteil des Recruiting-Prozesses. Die Software muss dann sowohl die datenschutzkonforme Bearbeitung der Bewerbungen unterstützen als auch generell den Anforderungen an Informationssicherheit genügen.

Die meisten Bewerbermanagement-Systeme sind heutzutage als „Cloud-Lösung“ im Betrieb, werden also nicht im Unternehmen selbst installiert, sondern beim Systemanbieter. Dann kommt dem ganzen Thema noch eine wichtigere Bedeutung zu, denn die Bewerberdaten liegen dann nicht bei dem Unternehmen, bei dem sich der Kandidat beworben hat, sondern beim Anbieter. Hier ist also noch einmal besonders darauf zu achten, dass die Software und der Anbieter selbst sowohl Datenschutz als auch Datensicherheit groß schreiben.
Ein guter Indikator hierfür ist die Zertifizierung des Anbieters nach DIN ISO 27001. Diese bringt die Aufgabe mit sich, für alle Daten innerhalb und außerhalb der Software höchste Integrität, Verfügbarkeit und Vertraulichkeit sicherzustellen. Ein Software-Anbieter, der nach ISO 27001 zertifiziert ist, kann also Risiken oder Vorfälle nicht ignorieren, sondern muss sich stets und zeitnah um Verbesserung der Informationssicherheit bemühen. Davon profitieren dann Recruiter in zweierlei Hinsicht: sie nutzen ein Bewerbermanagement-System, welches ständig überprüft und optimiert wird, und sind bei ihrem Recruiting-Prozess jederzeit rechtssicher unterwegs, solange sie ihre Abläufe innerhalb der Software umsetzen und einhalten.

Unser Tipp: Datenschutzthema frühzeitig im Blick haben!

Bei Neu-Einführung einer eRecruiting-Software ist es empfehlenswert, die in Frage kommenden Anbieter hinsichtlich dieser datenschutzrelevanten Themen frühzeitig „unter die Lupe zu nehmen“.
Je transparenter und klarer Sie Antworten zu diesem Thema erhalten, je einfacher gestaltet sich erfahrungsgemäß die interne Abstimmung mit Ihrem Datenschutzbeauftragten.
Im Idealfall können Detailfragen zu Datenschutz und Datensicherheit direkt zwischen dem Experten Ihres Unternehmens und dem Datenschutzverantwortlichen des Systemanbieters geklärt werden. Dann steht einer schnellen und unkomplizierten Nutzung des Bewerbermanagement-Systems nichts mehr im Wege!

Funktionen, die Ihr Bewerbermanagement-System haben sollte

- ☐ Funktionen zur manuellen Löschung von Bewerberdaten
- ☐ Möglichkeit, individuelle Datenschutztexte und Löschfristen zu definieren
- ☐ Integration von Fachbereichen, Betriebsräten und anderen Parteien des Bewerbungsprozesses im System, so dass Bewerberdaten komplett innerhalb des Systems „versendet" werden können
- ☐ klares Benutzerrollen- und Rechtekonzept, mit der eindeutig und gleichzeitig flexibel geregelt werden kann, welcher Mitarbeiter welche Bewerbungen einsehen darf
- ☐ IP-basierte Zugriffsregeln, durch die das System ausschließlich aus dem firmeneigenen Netzwerk erreicht werden kann
- ☐ durchgehend verschlüsselte Datenübertragung (per https)
- ☐ eigene, separate Datenbanken pro Unternehmen

Tipps für einen datenschutzkonformen Bewerbungsprozess

- ✓ bei Online-Bewerbung über ein Formular: Kandidaten sollten vor dem Absenden des Formulars verpflichtend ihre Zustimmung zur Ihrer unternehmensindividuellen Datenschutzerklärung erteilen. Diese sollte mindestens über folgende Aspekte informieren:
  - ✓ Datenspeicherung und -verarbeitung gemäß deutschen Datenschutzbestimmungen
  - ✓ Vertrauliche Behandlung der Daten ausschließlich innerhalb des Unternehmens
  - ✓ Speicherung der Daten für einen festgelegten Zeitraum nach Abschluss des Bewerbungsverfahren.
- ✓ bei Bewerbung per E-Mail oder per Post: Kandidaten sollten über oben genannte Punkte informiert werden, sofern diese Bewerbungen ebenfalls digitalisiert und im Recruiting-System verarbeitet werden.
- ✓ klare Definition von Löschfristen im Bewerbermanagement-System, in Abhängigkeit des jeweiligen Status im Auswahlprozess (bspw. Löschung 6 Monate nach Absage, 1 Monat nach Einstellung). Diesen Löschfristen müssen die Bewerber im Rahmen der Datenschutzerklärung zustimmen!
- ✓ Unterlagen von Kandidaten, die explizit um Löschung ihrer Daten gebeten haben, müssen an allen vorliegenden Stellen umgehend gelöscht werden.
- ✓ Original-Bewerbungen sollten nach der Digitalisierung zurückgesendet oder vernichtet werden, um nicht-datenschutzkonforme Speicherung (in E-Mail-Postfächern oder Archiven) zu vermeiden.
- ✓ Bewerbungsunterlagen sollten ausschließlich innerhalb des Recruiting-Systems an definierte Fachbereiche weitergeleitet werden (kein Versand per E-Mail, keine Ausdrucke!).

Fragen an Anbieter eines cloudbasierten Recruiting-Systems

- √ Wer hat Zugriff auf Ihre Bewerberdaten und wie wird der Zugriff auf diese Daten überwacht?
- √ Hat Ihr Anbieter Auftragsdatenverarbeitungsverträge (ADV) mit seinen externen Dienstleistern abgeschlossen (z. B. Rechenzentren)?
- √ Wie erfolgt die Datensicherung Ihrer Bewerberdaten? Wie sieht die Backupstrategie aus?
- √ Gibt es Vorgaben zum Löschen der Bewerberdaten (inkl. Datenträgern)?
- √ Welche Sicherheitsrichtlinien gelten jeweils für Server, Datenbanken und Infrastruktur?
- √ Wie sehen die technisch-organisatorischen Maßnahmen (TOMs) beim System-Anbieter aus?
- √ Ist der System-Anbieter und/oder das Rechenzentrum zertifiziert?
- √ Liegt ein Auditbericht zum Thema „Datenschutz" für den Anbieter vor?
- √ Werden Risikobewertungen durchgeführt, um Risiken frühzeitig zu erkennen und vorzugehen?
- √ Werden Pentests durchgeführt, um Schwachstellen in der Software oder Infrastruktur festzustellen?
- √ Gibt es ein Incidentmanagement, um Sicherheitsvorfälle zu beheben und zukünftig vorzubeugen?
- √ Wie ist die Haftung des Anbieters im Schadensfall geregelt?
- √ Wie sieht die Informationssicherheitspolitik des Anbieters aus und gibt es Informationssicherheitsziele?
- √ Gibt es einen Datenschutzbeauftragten, der auch datenschutzrelevante Anfragen seitens der Unternehmen beantworten/klären kann?

Sie haben noch Fragen zum Thema Datenschutz bei d.vinci? Zögern Sie nicht und kontaktieren Sie uns!

d.vinci Recruitinglösungen
Team Consulting

Tel.: +49 (0) 40-37 47 99 0
E-Mail: Kontakt@dvinci.de