Recruiting-Checkliste DSGVO

Die Datenschutzgrundverordnung (DSGVO) stellt an den Recruiting-Prozess hohe Anforderungen. Mit unserer Checkliste halten Sie alle elementaren Vorgaben zuverlässig ein.

1. Datenschutzkonformes Löschen personenbezogener Daten

Sämtliche Bewerberdaten müssen unverzüglich gelöscht werden, sobald der Recruiting-Prozess abgeschlossen ist. Dazu stellen Sie folgendes sicher:

- ☐ Alle Daten werden digital verwaltet
- ☐ Für eine bessere Auffindbarkeit sind alle Daten zentral abgelegt
- ☐ Alle Systeme, mit denen personenbezogene Daten verarbeitet werden, sind bekannt
- ☐ Sie haben Zugriff auf sämtliche Daten und können diese bei Bedarf vollständig löschen
- ☐ Die Löschung aller Daten erfolgt fristgerecht und im Optimalfall automatisch
- ☐ Werden Daten in Ausnahmefällen – zum Beispiel bei Rechtsstreitigkeiten – länger gespeichert, wird der Bewerber über die verlängerte Datenaufbewahrungsfrist und die Gründe dafür informiert
- ☐ Die Informationen werden dem Bewerber unverzüglich schriftlich per E-Mail zugestellt

2. Informationspflicht des Arbeitgebers

Unternehmen sind verpflichtet, Talente nach Eingang einer Bewerbung über die Dauer und Art und Weise der Speicherung ihrer Daten zu informieren

- ☐ Ein Standardschreiben, das über Rechtsgrundlagen, Zwecke, Löschfristen und sämtliche Daten, die im Bewerbungsprozess erhoben werden, ist erstellt.
- ☐ Talente erhalten die Informationen direkt nach Absenden ihrer Bewerberunterlagen per E-Mail.
- ☐ Ein automatisierter Versandprozess stellt dies zuverlässig sicher.
- ☐ Er beinhaltet eine automatische Abfrage zur Einwilligung in die Datenverarbeitung.
- ☐ Die Einwilligung von Bewerbern in die Datenverarbeitung wird automatisch in der Bewerberakte abgelegt.
- ☐ Der Verarbeitungsprozess erfolgt erst nach Erhalt der Einwilligungserklärung.

3. Auskunftsrecht des Bewerbers

Talente haben das Recht, bei einem Arbeitgeber eine Auskunft über die Daten einzuholen, die er über sie vorhält.

- ☐ Die Auskunft erfolgt ohne jeden zeitlichen Verzug und vollständig
- ☐ Das eingesetzte Recruiting-System verfügt über eine Funktion, mit der jederzeit eine Kopie des kompletten gespeicherten Datensatzes erstellt werden kann
- ☐ Über eine Exportfunktion lesen Anwender Informationen zu einem Bewerber auch aus anderen Systemen aus
- ☐ Der Bewerber erhält die Informationen über einen verschlüsselten Datentransfer

4. Verpflichtung zur Datensicherheit

Wer Daten vorhält, ist verpflichtet, diese nach geltenden Standards der IT-Security aufzubewahren. Das ist zu beachten:

- ☐ Sämtliche Daten werden innerhalb der EU gehostet
- ☐ Das Rechenzentrum, in dem Daten gespeichert werden, verfügt über Sicherheitszertifikate, die die Einhaltung aller gültigen IT-Security Richtlinien belegen.
- ☐ Die ISO-Norm 27001 steht für höchste Sicherheits-Standards
- ☐ Der Anbieter eines Bewerbermanagementsystems führt regelmäßige Sicherheitstests durch
- ☐ Den Nachweis darüber erbringt er über ein aktuelles Penetrationstest-Zertifikat.

5. Die Frage der Haftung

Anwender eines Bewerbermanagementsystems haften im Falle eines Verstoßes gegen den Datenschutz genauso wie der externe Dienstleister. Was ist zu beachten?

- ☐ Sie haben sich überzeugt, dass alle Prozesse DSGVO-konform gesteuert werden
- ☐ Der Auftragsdatenverarbeitungsvertrag des Anbieters liegt vor
- ☐ Er führt alle technischen und organisatorischen Abläufe innerhalb des Rechenzentrums auf
- ☐ Er regelt explizit Auftraggeber- und Auftragnehmerpflichten
- ☐ Der externe Partner lässt alle Prozesse von einem Datenschutzbeauftragten prüfen
- ☐ Der Lösungsanbieter listet in einer Datenschutzerklärung nachvollziehbar auf, inwiefern die Sicherheit aller vorgehaltenen Daten gewährleistet wird.
- ☐ Ihr Datenschutzbeauftragter hat den Einsatz des Systems nach eingehender Prüfung für unbedenklich erklärt

6. Funktionen zum Datenschutz innerhalb des Bewerbermanagementsystems

Innerhalb des eigenen Unternehmens dürfen Daten nicht in unberechtigte Hände fallen. Dafür sollte das eingesetzte Bewerbermanagementsystem über folgenden Funktionen verfügen:

- ☐ Individuelle Zugriffsrechte für verschiedene Nutzerprofile
- ☐ Limitierte Zugriffsrechte für Betriebsräte
- ☐ Automatische Dokumentation geänderter Zugriffsrechte
- ☐ Automatische Meldung von potenziellem Datenmissbrauch
- ☐ Prozesse zur Daten-Wiederherstellung
- ☐ Sichere Backups aller Daten