

Datenschutzkonformes E-Recruiting

Mitarbeitersuche 2.0

E-Recruiting beginnt bei Stellenanzeigen im Internet und reicht von der Stellenausschreibung in Jobportalen bis hin zur Online-Anwendung im „Karriere“-Bereich Ihrer Unternehmens-Website. In tatsächlicher Hinsicht ist das Online-Recruiting für beide Parteien praktisch. In rechtlicher Hinsicht ist es jedoch besonders sensibel, weil hier persönlichkeits- und datenschutzrechtliche Belange gleichermaßen berührt werden. Sichern Sie sich daher mit einer Checkliste ab.

► Bereits jedes vierte Unternehmen erhält Bewerbungen am liebsten elektronisch. Das ergab eine Erhebung des BITKOM vom April 2010. Insgesamt 27 Prozent der befragten Firmen bevorzugen eine Kontaktaufnahme per E-Mail oder Web-Formular.

Reine Bewerberdaten dürfen Sie ohne Einwilligung erheben

Die Erhebung von personenbezogenen Daten eines Bewerbers ist als Entscheidungsgrundlage für die Begründung eines Arbeitsverhältnisses erforderlich. Damit ist sie nach § 32 Abs. 1 S. 1 BDSG zulässig. Im Regelfall benötigen Sie auch keine elektronische Einwilligung (nach § 4a BDSG).

Beachten Sie das TMG

Da entsprechende Internet-Portale und Online-Anwendungen als Telemedien im Sinne des Telemediengesetzes (TMG) einzuordnen sind, müssen Sie neben den Regelungen des BDSG auch die §§ 11 bis 15 TMG beachten.

Anforderungen an datenschutzgerechte Recruiting-Portale

Aus datenschutzrechtlicher Perspektive müssen Sie im Rahmen von E-Recruiting-Portalen und entsprechenden Anwendungen insbesondere die folgenden datenschutzrechtlichen Anforderungen beachten:

- Unterrichtung des Nutzers/Bewerbers
- technisch-organisatorische Sicherungsmaßnahmen im Bewerbungsprozess

- besondere Pflichten bei Einschaltung von externen Dienstleistern
- Löschungspflichten und Aufbewahrungsfristen von Bewerberdaten



Wer online Jobs anbietet, muss ein besonderes Augenmerk auf den Datenschutz haben

Ihre Unterrichtspflichten

Der Online-Bewerber ist nach § 4 Abs. 3 BDSG über die – in datenschutzrechtlicher Hinsicht – verantwortliche Stelle und die Empfängerkategorien zu unterrichten.

Darüber hinaus muss der Online-Bewerber durch den für den Teledienst Verantwortlichen nach § 13 Abs. 1 TMG darüber informiert werden, wenn seine Daten in einem Drittland verarbeitet werden. Gleiches gilt, wenn er durch automatisierte Verfahren identifiziert werden kann.

Stellen Sie Identität und Integrität der Bewerberdaten sicher

Wie bei jeder Datenverarbeitung gilt es auch beim Online-Recruiting, durch technisch-organisatorische Sicherungsmaßnahmen die Identität und Integrität der Daten sicherzustellen.

Datenübertragung nur mit SSL-Verschlüsselung

Von besonderer Bedeutung ist dabei Ziffer 4 der Anlage zu § 9 BDSG: Personenbezogene Daten dürfen während der elektronischen Übertragung bzw. ihres Transports weder unbefugt gelesen, kopiert oder verändert noch unbemerkt entfernt werden. Dies gilt umso mehr angesichts der persönlichkeitsrechtlichen Bedeutung von Bewerberdaten.

Folglich dürfen Bewerberdaten nur über eine sichere Verbindung – also mittels SSL-Verschlüsselung – übertragen werden.

Dienstleister sind Auftragsdatenverarbeiter!

Werden die Bewerberdaten durch einen externen Dienstleister verarbeitet, müssen Sie besondere Anforderungen beachten. Dies ist etwa der Fall, wenn die Recruiting-Anwendung nicht vom Unternehmen selbst betrieben wird, sondern durch einen Service Provider. Regelmäßig liegt dann eine Auftragsdatenverarbeitung nach § 11 BDSG mit den entsprechenden Folgen vor.

Fixieren Sie den Anforderungskatalog an den Auftragnehmer schriftlich

§ 11 BDSG sieht nach der BDSG-Novelle insbesondere vor, dass der Anforderungskatalog der Auftragsdatenverarbeitung schriftlich fixiert wird. Dazu zählen u.a. Regelungen

- zur Berichtigung, Sperrung oder Löschung von Daten,
- zu den zu treffenden technischen und organisatorischen Maßnahmen,
- zu den Kontrollrechten des Auftraggebers oder
- zum Umfang der Weisungsbefugnisse.

Speichern Sie Bewerberdaten höchstens ein halbes Jahr

Während der Dauer des laufenden Anbahnungs- und Abwicklungsverhält-

„Wasserdicht“ organisieren

nisses im Bewerbungsprozess dürfen die Daten drei bis sechs Monate aufbewahrt werden.

Auf Widerspruch hinweisen

Sollen sie darüber hinaus gespeichert werden, um den Bewerber zu einem späteren Zeitpunkt noch einmal anzusprechen, müssen Sie den Bewerber darüber informieren. Vergessen Sie dabei nicht den Hinweis auf die Widerspruchsmöglichkeit!

Bewerberdaten sauber löschen

Achten Sie beim Löschen von Bewerberdaten darauf, dass das Löschen unternehmensweit – und gegebenenfalls bis hin zum Dienstleister – erfolgen

muss. Stellen Sie also intern sicher, dass Abteilungen, denen die Bewerbungsunterlagen digital zur Verfügung gestellt wurden, eventuell vorhandene Kopien ebenfalls löschen.

Sorgsamer Umgang mit Bewerberdaten ist ein wichtiger Datenschutz-Baustein

Nicht nur aufgrund der datenschutzrechtlichen Bedeutung, sondern gerade auch wegen der persönlichkeitsrechtlichen Relevanz gilt es, mit Bewerberdaten sorgsam umzugehen.

Daher stellt die datenschutzkonforme Ausformung des E-Recruiting-Prozesses einen wesentlichen Baustein im unternehmerischen Datenschutz dar.

In den Prozess sind sowohl Sie als Datenschutzbeauftragter (insbesondere im Hinblick auf das Verfahrensverzeichnis) sowie gegebenenfalls auch der Betriebsrat einzuschalten. Das ist beispielsweise bei internen Ausschreibungen der Fall.

Checkliste abarbeiten und nichts vergessen

Stellen Sie sicher, dass Sie im Rahmen des E-Recruitings nichts übersehen – die Checkliste auf dieser Seite hilft Ihnen dabei!

Peer Lambertz

Peer Lambertz ist Rechtsanwalt und Datenschutzexperte.

Fragestellung	Ja	Handlungsbedarf
1. Kann der Bewerber klar erkennen, wer Empfänger seiner Daten und wer verantwortliche Stelle für die Datenerhebung und -verarbeitung ist?	<input type="checkbox"/>	<input type="checkbox"/>
2. Wird ggf. auf eine Verarbeitung in Drittländern hingewiesen?	<input type="checkbox"/>	<input type="checkbox"/>
3. Gibt es neben spezifischen Stellenausschreibungen auch die Möglichkeit der Initiativbewerbung? Wird in diesem Fall auf abweichende Aufbewahrungs- und Löschrufen hingewiesen?	<input type="checkbox"/>	<input type="checkbox"/>
4. Existiert für die Bearbeitung einer Online-Bewerbung ein definierter Unternehmens- bzw. Konzernprozess, der den technisch-organisatorischen Sicherungsmaßnahmen gemäß Anlage zu § 9 BDSG gerecht wird (bspw. Zugriffsbeschränkung auf Datenbanken oder Protokollierung von Kopien der Bewerberdaten und -unterlagen einschließlich der unternehmens-/konzernweiten Datenlöschung)?	<input type="checkbox"/>	<input type="checkbox"/>
5. Sofern der Online-Bewerbungsprozess über eine Online-Recruiting-Anwendung abgewickelt wird: Können dort sensible Daten wie Lebensläufe oder Zeugnisse über eine sichere Verbindung (per SSL) hochgeladen werden?	<input type="checkbox"/>	<input type="checkbox"/>
6. Sofern bei Online-Bewerbungen keine sichere SSL-Verbindung zum Einsatz kommt: Ist (neben einer E-Mail-Adresse) eine postalische Anschrift angegeben?	<input type="checkbox"/>	<input type="checkbox"/>
7. Werden ggf. automatische Filter im Rahmen des Online-Bewerbungsprozesses gesetzt, um Bewerbungen zu selektieren, und genügen sie den Anforderungen aus § 6a, § 28b BDSG (keine rein automatische Einzelfallentscheidung im Rahmen von Scoring-Verfahren)?	<input type="checkbox"/>	<input type="checkbox"/>
8. Sofern Bewerberdaten über einen längeren Zeitraum vorgehalten werden sollen: Wird darauf erkennbar hingewiesen und über die Widerspruchsmöglichkeit unterrichtet?	<input type="checkbox"/>	<input type="checkbox"/>
9. Werden die Bewerberdaten – insbesondere auch nach der initialen Verbindung – mittels einer sicheren Verbindung übertragen und transportiert?	<input type="checkbox"/>	<input type="checkbox"/>
10. Werden beim Outsourcing im Rahmen des E-Recruitings die Vorgaben aus § 11 BDSG (Auftragsdatenverarbeitung) beachtet (insbesondere im Hinblick auf die ausdrückliche vertragliche Regelung des Anforderungskatalogs)?	<input type="checkbox"/>	<input type="checkbox"/>

Checkliste E-Recruiting. Die Checkliste finden Sie online zum Download im Word-Format unter <http://www.datenschutz-praxis.de/fachwissen/vorlagen/checklisten>.