Die Dos und Don’ts beim Datenschutz im Recruiting

Wie Recruiting-Software aus der Cloud dabei hilft, Such- und Bewerbungsprozesse DS-GVO-konform zu optimieren.

Spätestens seit die Europäische Datenschutz-Grundverordnung EU-DS-GVO in Kraft getreten ist, gilt: Wer Recruiting betreibt, muss den Datenschutz nicht nur zuverlässig einhalten, sondern das auch rechtssicher dokumentieren und bei Bedarf jederzeit nachweisen können. Wenig überraschend kann dies umso besser gelingen, je klarer die Recruiting-Prozesse strukturiert sind und deren Einhaltung softwaretechnisch sichergestellt wird.

Aber bei näherer Betrachtung leistet selbst Cloud-Technologie einen wertvollen Beitrag, wenn sie denn richtig eingesetzt wird. Die wichtigsten Empfehlungen im Überblick.

1. Nicht auf lokale Daten verlassen

Auf meinem persönlichen Computer sind doch alle Daten sicher! So zumindest sehen das wohl diejenigen Recruiting-Verantwortlichen, die sich bei der Organisation ihrer Arbeit auf lokale Dateien wie Excel-Tabellen und Word-Dokumente verlassen. Auch wer serverbasierte Recruiting-Software verwendet, die eine Replikation ihrer Datenbank mit den Clients vornimmt, hat das identische Problem: Am Ende trägt man auf persönlichen Geräten wie Laptop, Tablet oder Smartphone vertrauliche Personendaten lokal gespeichert stets bei sich.

Dass das keine gute Idee ist, verdeutlichen beispielsweise die Meldungen der Flughäfen: Allein in Frankfurt kommen pro Woche 300 Laptops durch Diebstahl und – vor allem – Vergessen in der Sicherheitskontrolle abhanden. Jeder einzelne Verlust, bei dem sich Bewerberdaten auf dem Gerät befinden, ist ein meldepflichtiger Datenschutzvorfall. Das ist nicht nur unangenehm, sondern auch aufwendig: Waren die Daten nicht verschlüsselt, muss neben der Aufsichtsbehörde nämlich jeder Betroffene einzeln informiert werden.

Schon deshalb sollten Schutzmaßnahmen wie sichere Datenverschlüsselung und Zugangsbeschränkung per Zwei-Faktor-Authentifizierung über physische Sicherheitsmerkmale wie einen USB- oder NFC-Token selbstverständlich sein. Trotzdem bleiben Sicherheitslücken – etwa ein unverschlüsseltes Backup, das in die falschen Hände gerät, ein Handwerker, der sich bei der Arbeit im Büro Zugang zu den Daten verschaffen kann, oder ein Hackerangriff. Der Rat muss daher lauten, möglichst wenig Daten lokal zu speichern.

2. Server: aber sicher!

Ist eine Server-Lösung also sicherer? Wenn der Server ein gewöhnlicher PC ist und einfach irgendwo im Büro steht, wo gerade Platz ist – vielleicht gar in den Sanitärräumen oder im Wartebereich – dann sicher nicht. Wer sogenannte gehärtete Server-Räume zur Verfügung hat und darin ein professionelles Management seiner Server gewährleisten kann, bringt hingegen bessere Voraussetzungen mit, allerdings auch zu erheblich höheren Kosten.

„Gehärtet“ müssen dann jedoch nicht nur die Räume, sondern auch die Sicherheitskonzepte sein. Seit einiger Zeit häufen sich etwa neuartige Hacker-Angriffe, die Daten abschöpfen oder verschlüsseln und erst gegen Lösegeld wieder freigeben. Meist genügt der Befall eines einzigen Arbeitsplatzrechners, damit sich die Schadsoftware im ganzen Unternehmen ausbreiten kann. Dann sind grundsätzlich auch alle Datensicherungen betroffen, die über das lokale Netzwerk erreichbar sind.

Auf Nummer sicher geht also nur, wer seinen Server nicht in eigenen Räumen betreibt, sondern in externen Rechenzentren mit geografischer Redundanz betreiben lässt.

3. Die Cloud kann helfen

Solche hochsicheren Rechenzentren finden sich primär bei den Cloud-Anbietern. Grundsätzlich ist der Betrieb von Recruiting-Lösungen aus der Cloud auch gar keine schlechte Idee. Die Sicherheit der Rechenzentren steht außer Zweifel, auch ein Einbruch ins Büro und selbst ein erfolgreicher Hackerangriff auf das eigene Netzwerk lassen sich verschmerzen: Neue Arbeitsplatzrechner sind schnell organisiert und mit einer Browser-

Lösung kann notfalls auch im Internet-Café nebenan weitergearbeitet werden.

Ungemach droht hier allerdings von anderer Seite: Der Server-Standort muss unbedingt innerhalb des Gültigkeitsbereichs der DS-GVO, also in der EU liegen. Ein Datentransfer in Drittstaaten – etwa die USA – muss technisch wie rechtlich ausgeschlossen sein, um sich nicht auf juristisches Glatteis zu begeben.

Aus diesem Grund sind auch gängige Cloud-Speicher wie Dropbox, WeTransfer oder OneDrive absolut tabu. Wer darüber beispielsweise Bewerberprofile an Auftraggeber überträgt, begeht bereits einen Bruch des Datenschutzes. Selbst eine Terminabstimmung per Doodle oder ähnlichen Diensten ist nicht zulässig, sobald im Termineintrag persönliche Daten, etwa der Bewerbername oder auch nur dessen Mail-Adresse, zu lesen sind. Verantwortungsvolle Anbieter von Recruiting-Software aus der Cloud realisieren stattdessen rechtssichere eigene Angebote, die in Europa gehostet werden, deutschem Recht unterliegen und den Datenschutz uneingeschränkt gewährleisten.

4. Vorsicht mit E-Mails

Als Gefahr für den Datenschutz weithin unterschätzt wird die Verwendung von E-Mails. Hier liegen die Probleme gleich auf mehreren Ebenen: Zunächst einmal findet die Übertragung von E-Mails über das Internet unverschlüsselt im Klartext statt. Allein deshalb sollte sich dieser Kommunikationsweg für vertrauliche Informationen von selbst verbieten. Zudem bleiben die Inhalte einer Mail einschließlich aller Anhänge lokal bei Absender und Empfänger gespeichert, oft sogar zusätzlich noch auf dem Server des Providers. Und natürlich können Empfänger die Mail-Informationen weiterleiten – an fremde Personen, aber auch an einen eigenen privaten Mail-Account, beispielsweise durch Weiterleitungsregeln bei Abwesenheit vom Büro.

Mit professionellen E-Mail-Systemen, wie Microsoft Exchange, lassen sich einige dieser Problempunkte eliminieren – beispielsweise durch verschlüsselte Übertragung, eine E-Mail-Policy, die notfalls das Fernlöschen von E-Mails auf dem Client ermöglicht, und natürlich eine Beschränkung des E-Mail-Hostings auf sichere Server innerhalb der EU. Trotzdem entstehen bei der Weiterleitung an fremde E-Mail-Systeme unkontrollierbare Daten-Kopien und auch der eingehende E-Mail-Verkehr legt mindestens einen Teil der Strecke durch das öffentliche Internet zurück.

Wo immer möglich sollte deshalb auf den Einsatz von E-Mails verzichtet werden. Mit entsprechender Recruiting-Software können Kandidaten ihre Bewerbungsunterlagen verschlüsselt direkt im Browser hochladen. Statt per Mail-Kopie der Original-Unterlagen werden Auftraggeber kontrolliert über ein Client-Center informiert, das vertrauliche Unterlagen nur zur temporären Ansicht und wahlweise auch anonymisiert zur Verfügung stellt. Unangefordert per Mail eingehende Daten werden in die Datenbank übernommen und dort mit klarem Bezug zum Projekt und dem Kandidaten abgespeichert.

5. Bloß nicht ärgern lassen

Nur so ist zu leisten, was das Gesetz fordert: Nämlich, dass ein Kandidat jederzeit Auskunft erhalten kann, welche Daten von ihm überhaupt vorliegen und auf welcher Rechtsgrundlage diese gespeichert sind. Dann wird es auch wichtig, nachzuweisen, dass er seine Zustimmung zur Datenspeicherung erteilt hat – etwa per sauber dokumentiertem Double-Opt-in-Verfahren.

Und was, wenn jemand seine Zustimmung nachträglich zurückzieht? Überhaupt müssen alle personenbezogenen Daten gelöscht werden, sobald sie nicht mehr zwingend benötigt werden. Wenn dann Bewerbungsanschreiben im Dateisystem auf dem Laptop, die weitere Korrespondenz im Mail-System, eine Excel-Übersicht aller Bewerber auf dem Server und die eingereichten Arbeitsnachweise als Grafik-Dateien in der Dropbox gespeichert sind, wird es schwierig.

Die richtige Software macht's

„Eine gute Recruiting-Lösung muss sämtliche anfallenden Prozesse optimal unterstützen. hunter-Anwender sind auch auf die Anforderungen des Datenschutzes bestens vorbereitet", weiß Gerhard Schickel, Head of Recruitment Solutions bei fecher. „Jeder Recruiter, dem das Auskunftsersuchen eines abgelehnten Bewerbers Kopfzerbrechen bereitet oder der bei einer Anfrage der Datenschutzbehörde überlegen muss, wie die Zustimmung zur Aufnahme in den Kandidatenpool belegt werden soll, hat heutzutage ein echtes Problem." Allerdings eines, das sich mit der sorgfältig gewählten Kombination aus Technologie und Anwendungslösung leicht lösen lässt.

MICHAEL IHRINGER,
freier Autor, ihringer@in-house.de