Featured in the National Association of Legal Search Consultants Summer 2024 Newsletter

Cybersecurity and Data Privacy – What Recruiters Need to Know*

by Diana Iketani Iorlano, Esq.

From personal information about candidates to confidential information about firms, recruiters often possess the most intimate details.

But what are recruiters' legal obligations to safeguard the information they receive in the course of their duties? How do you navigate the many privacy and confidentiality laws, especially when you operate in multiple jurisdictions or internationally? Can you safely share the information with others? Do you have obligations to delete the information? Should you be worried about data breaches?

At the recent NALSC Conference in San Diego, we touched on many of these topics in a well-attended breakout session. We recommended the steps below that recruiters, recruiting firms, and in-house recruiters can take to comply with applicable laws and be good stewards of personal and confidential information from candidates and firms.

Recruiters Should Implement Clear and Conspicuous Privacy Policies

All recruiting businesses should create and implement a Privacy Policy that states how the company collects/uses/shares personal information and provides a way for candidates/firms to assert their privacy rights. This may be required by law under the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or similar statutes. Your website privacy policy should plainly state what information you collect, the third parties with whom you may share the information, the retention period of the personal information, and any applicable methods for an individual to request deletion or modification of their personal information. This can show potential clients that you respect their privacy and are aware of the applicable laws relating to personal information. The Privacy Policy should also apply to information you may be collecting from website visitors – including disclosures about cookies and analytics that may be running on your website. With new privacy laws coming online nearly every month, privacy policies and practices should be reviewed at least annually to ensure they reflect how the company is handling personal information.

Data Mapping – Taking Stock of What Information You Have

Consider what personal and confidential information you or your firm may collect. Recruiters have access to detailed personal information, such as the candidate's name, address, email/phone contacts, educational information, prior workplace information, family information (e.g., dependents, including minors), and client lists, as well as categories of sensitive personal information that may require additional protection: gender, race, sexual orientation, SSN, health conditions, disability status, veteran/military status, financials, and background check information including criminal or credit information. Similarly, recruiters may have confidential information from a firm or organization, including the firm's financial performance, profits per partner, partner/C-suite contact information, client lists, acquisition or merger information, market analyses, and other non-public information.

> *"In general, the more public the information is, the less protection it gets."*

It's essential to implement a comprehensive data map to understand what types of information your organization collects. The data map should list the sources of information, the fields of information collected, the storage mechanism for the data (are you using third-party software, an Excel spreadsheet or handwritten notes?), any downstream recipients of the information (consultants, software, vendors), and retention periods for the information. With nearly unlimited digital storage, we can keep data forever, but we shouldn't.

Cybersecurity and Privacy Training are Essential

Similarly, access to personal information should be limited to those who need it and those who have access to personal information should be trained in how to protect it. Can you limit access to personal information to only those who need it? When nearly 88% of data breach incidents come as a result of employee mistakes, it makes sense to minimize how long data is kept and who has access to it. In addition, vendors or service providers that have access to candidate personal data should be engaged with written agreements that include confidentiality provisions and require adherence to privacy laws.

The source of the information may also matter. Are you receiving information from publicly available sources or are you getting the inside scoop from a confidential source or the candidates themselves? Are you collecting this personal information through phone calls, emails, webforms on your website, third-party sites like LinkedIn and Indeed, or from other third parties, such as other candidates or other recruiters?

In general, the more public the information is, the less protection it gets, but gone are the days when you could assume that a candidate's business information wasn't protected. In some jurisdictions, business information is treated the same as personal information, so a business email address might be entitled to the same protection as the candidate's personal email address. If you are collecting information through webforms, are they secure? Do you have multifactor authentication on your accounts? Where do you store personal information (on the cloud? on your laptop?) and is it password protected?

Privacy laws require you to implement reasonable technical and security measures to protect information in your possession. Talk to your

Continued on next page

Continued from prior page

IT team or invest in a consultant to review the cybersecurity measures in place to protect personal information. Do you have cyberinsurance that will protect you in the event of a data breach or ransomware event? What does it cover? Do you have a business continuity and incident response plan in the event of a security incident? Who will you call if information in your possession is breached?

Implement Principles of Data Minimization

Given the high risk of exposing candidate personal information or firm confidential information or the PR nightmare of a data breach, recruiters should implement a data retention policy to minimize the length of time personal information is kept after candidate consideration or placement and/or encrypt data that is especially sensitive. Think of how you would want your personal information to be protected if you were a candidate or the firm that provided its financials to you. Would you want to inform a prospective candidate from 15 years ago that you held their information indefinitely and it was breached? Data breach notification laws may require just that.

Conclusion

Data privacy is here to stay, and compliance is essential for companies that handle personal information. Regardless of where your privacy program currently stands, you will be expected to know and comply with applicable privacy and security laws. It's essential to get it right the first time – you might not have another chance!

**The information in this article is for general educational purposes only and should not be construed as legal advice.*

ABOUT THE AUTHOR:

Diana Iketani Iorlano, Esq. is the Founder/Managing Attorney of Iketani Law Corporation, a Los Angeles boutique focusing on data privacy and cybersecurity compliance. Prior to founding Iketani Law, Ms. Iketani served as the Chief Recruiting Officer for an AmLaw 200 firm.

P: (310) 627-2752
E: diana@iketanilaw.com
W: www.iketanilaw.com