

Keeping Job Applications Secure

The importance of secure collaboration on job application documents

Résumés are categorized as personal data and must be protected, according to the European Union's Directive 95/46/EC, which also applies to US-based firms adhering to Safe Harbor principles. As a result, companies may need to rethink how they store and work with candidates' job applications. They must ensure that this information is protected from access by unauthorized people and that it cannot be intercepted while circulating between the HR and line-of-business departments. Logging every access to the documents, as well as all comments, helps speed the selection process while providing more transparency and security. This may sound obvious, but incidents in the past have shown that companies can suffer considerable damage if word gets out that they have been careless with candidates' personal data. In fact, the impact on their image may cost them more than any disciplinary action resulting from a violation of data protection laws.

Risks in handling job candidates' personal data

The days when job applications arrived by postal mail in carefully-prepared folders are long gone. Today, companies are more interested in quickly pinpointing the best candidate from a pile of applications – before their competitors get there first. This means they need the documents in digital format that they can be shared with other companies. Not all firms have an efficient workflow system that quickly forwards documents on to the right recipient. And even if they do, will the system support compliance requirements for data protection and traceability during the whole document handling process?

Experience has shown that compliance vulnerabilities start to appear when job applications need to be reviewed by staff outside the usual workflow – for example, in a distant subsidiary. To say nothing of what happens when resumes are shared with external

advisors like recruitment firms or lawyers. The usual way of sharing job applications – sending them as a non-secure email attachment – clearly contravenes compliance requirements. It's all too easy to type the wrong name into an email's "To" field or to forward and print the résumé and leaving it lying around for all to see. Also, the only way of ensuring the proven deletion of all copies of a document is with a logging function that tracks every action in its lifecycle until it is definitively archived or deleted.

Midsized and large companies around the world have been fulfilling these requirements for many years using Brainloop's Document Compliance solution. Brainloop makes it easy for HR departments to receive and distribute candidates' job applications in a secure and automated manner and to delete them in accordance with data protection laws once the application process is complete.

THE BENEFITS OF BRAINLOOP'S HR SOLUTION FOR THE JOB APPLICATION PROCESS

- › Secure and traceable handling of all personal information
- › Encryption of all electronic communications with no need to implement certificates or keys
- › External third parties can easily work with the data without software or certificate installation
- › Fast setup without involving the IT department
- › Transparency and control over the entire process
- › Faster response due to automated notifications
- › Minimization of manual handling
- › Automatic deletion of documents in accordance with legal regulations
- › Meets compliance requirements

To summarize, the requirements include speed, flexibility, availability, controlled deletion, and traceability for every access and change to confidential documents while ensuring the highest levels of protection for them.



Securing the process

These are some of the ways companies share résumés and similar types of personal information:

- › Incoming email from an external recruitment consultant
- › Incoming email directly from the candidate
- › Application via a web portal – usually unencrypted
- › Data shared by email with internal LOB and/or HR departments – unprotected
- › Data shared by email with external third parties such as lawyers – unprotected

With the Brainloop solution, candidate-related documents are encrypted and access to them is restricted to authorized personnel who are given the relevant permissions to view them.

This ensures compliance with legal and company-internal regulations concerning controlled and secure information handling, the deletion of the documents at the right time, and the traceability of the entire process.

Benefits of a Document Compliance solution

The Brainloop solution provides the highest levels of security because the



résumé and associated information is always encrypted – while it's being shared as well as when it's in storage. If desired, the documents can be delivered with a personalized watermark or with Digital Rights Management which build access limitations into the document while it's being created. These technologies can be used to stop a document from being printed or forwarded.

They also ensure that unauthorized staff – both internal and employees of external IT service providers and operators – will never be able to view confidential résumés and job applications. At the same time, it is very easy to include people from other departments or external business partners in the candidate review

process – without any software installation or training needed for those involved. They simply receive a link by email that gives them access to the confidential résumé from the candidate. To open the document, they first complete a two-factor authorization process by entering a password as well as a one-time PIN code that is sent automatically to their cell phone. The automated alerts sent to people involved in the candidate review accelerate response times and increases the efficiency of the whole selection process.

CONTACT

Brainloop, with offices in Munich and Boston, is the leading provider of Document Compliance Management solutions that enable customers to share confidential documents in a highly secure and traceable environment.

For more information please visit www.brainloop.com

Europe
Brainloop AG
 Franziskanerstr. 14
 81669 Munich · Germany
 T: +49 (89) 444 699 0
info@brainloop.de
www.brainloop.de

USA
Brainloop Inc.
 One Broadway, 14th floor
 Cambridge, MA 02142 · USA
 T: +1 (800) 517 3171
info@brainloop.com
www.brainloop.com

