

# The Importance of Protecting Employee Data



InfoGov Insights

# The Challenge: Protecting Employee Personal Information

In the last few years, the rise of regulations like GDPR and CCPA as well as the formalization of standards like ISO-27001 and ISO-27701 have made stringent data privacy protection a mandatory cost of doing business. Organizations around the world have adopted new technologies, new processes, and a greater level of transparency to meet these requirements in the face of sometimes very public incidents that have resulted in sensitive data loss or misuse.

Often overlooked in the ongoing dialog on data privacy protection is an acknowledgment that the data requiring oversight is not limited to customer or prospect data. Employee data is likewise an essential area of privacy protection, and indeed the GDPR mandate explicitly calls out employees as one of the data subject types accorded the rights of data disclosure, deletion, or modification by processor organizations.

## Areas of Vulnerability for Employee PII

While employee data privacy benefits from many of the process and technology investments made to protect customer data, there remain uses cases that are often overlooked by organizations focused primarily on the privacy of external data subjects.



## Recruitment and Onboarding



The typical recruitment process, especially in small to medium businesses, is one that is plagued with the sharing of candidates personally identifiable information. In a typical organization, candidates submit their CV using a web form or shared email inbox or distribution list. Upon receiving the CV and validating its match against the open position's requirements, the CV is usually sent via email as an attachment to a range of stakeholders associated with the vacancy. A new candidate applying for a role in an area such as product management, for instance, might see their CV sent to multiple stakeholders in engineering, sales, marketing, and support for their review and feedback.

This practice may have seemed innocuous enough until recently. In the world of GDPR, CCPA, and other employee/candidate data privacy protections, it is completely unacceptable. Embedded in that candidate's CV is personal information that may include their contact details, past job histories, contact information for personal or professional references, and even past earnings information. Perhaps even more troubling, 88% of respondents to a recent Ponemon study indicated that they received sensitive information via email that they weren't supposed to receive<sup>1</sup>.

Seeing this information duplicated across multiple email accounts, multiple attachments, and multiple devices clearly presents a data

1. <https://www.helpnetsecurity.com/2019/10/01/workplace-data-breaches-risk/>

a data privacy incident waiting to happen. More troubling than the possibility of an external breach, a misuse of sensitive data may even be initiated from within. Recent studies and incident investigations have revealed that other employees are often a source for the leakage of personally identifiable information (PII)<sup>2</sup>. For these reasons, the recruitment process is one that would benefit from a more stringent set of processes and tools aimed at data privacy protection.

### **Employee Credential Verification**



Employee credential verification is a routinely performed process in which current or former employees (or third-parties acting on their behalf, such as a bank or prospective employer) submit requests to an organization's HR team to provide details on job title, income history, dates of employment, and other information related to that employee's tenure.


As with recruitment and onboarding, in many organizations, this process is one that is heavily reliant on infrastructure and processes that are inherently insecure. Human resources staff often communicate credential verifications via email attachments, facsimiles, and other mediums that proliferate in unanticipated ways. Further, the information provided may be composed of both letters of verification as well as supporting documents like paystubs, etc.

The problems with this approach are manifold and include the

2. <https://www.cnn.com/2019/12/17/hacker-behind-your-companys-data-breach-may-be-in-the-next-cubicle.html>

distribution of document attachments containing sensitive information in a manner that puts them outside the control of Human Resources or the employee. By handling of this process in ways that restrict employee consent and visibility, and performing this work in a way that does not allow the employee to verify and (if needed) correct the information, Human Resources teams often inadvertently expose that sensitive data to misuse.

### Operational Disclosures

Challenges like the recent  COVID-19 outbreak have brought the potential for further slippage in employee data privacy protection, as noted in a recent article by the Wall Street Journal<sup>3</sup>. Employers trying to ensure the safety of their workforce have been (with the best of intentions) requiring employees to undergo medical screenings and to share that information with Human Resources as a condition of returning to the office. Once more, email and other inherently insecure communication channels are often the mediums by which this sensitive information is shared, creating the likelihood that information is saved off in insecure ways – local devices, insecure file shares, etc.

Aside from the crises posed by COVID-19 there are other operational issues. Perhaps the least understood of all, inadvertent and seemingly innocuous operational disclosures can lead to the unintended sharing of employee personal data. As part of

3. <https://www.wsj.com/articles/companies-walk-fine-line-on-employee-data-amid-coronavirus-outbreak-11583948984>

day-to-day communications, teammates and even Human Resources can with the best intentions share information that can be misused.

Something as simple as sharing an email celebrating an employee's birthday via a company-wide email, sharing the status of an employee who is taking time off work due to a medical issue, and other innocent disclosures must be looked at in a new light in the wake of increased protection of private, personal information.

For these reasons, the operational sharing of PII to ensure employee suitability for work or even share employee news needs to be reexamined from a process and technology perspective.

## Strategies for Better Securing Employee PII

Now that we have an understanding of some of the areas in which employee and job candidate data is at risk, let's look at some effective mitigation strategies.

### **More Secure Onboarding**



Onboarding efforts should focus on eliminating the use of potentially insecure systems for storing employee information. Too often, HR teams rely on shared servers, file shares, and groupware platforms that have not been configured to ensure secure storage – allowing unauthorized user roles or groups to have access to material that should be confidential. For this reason, file attachments containing new employee personal information should be stored only in HRM platforms accessible only by qualified

Human Resources personnel, or in groupware platforms like SharePoint that been appropriately access-controlled.

Operationally, Human Resources and Management team members should also be informed about the potential misuse of such seemingly trivial personal information and instructed to avoid the practice of sending birthday announcements, updates on the status of sick colleagues, or other information that has the potential to compromise privacy or be misused.

Solutions like the Information Governance Suite from Nyxeia are powerful enablers of more compliant HR practices. The .discover product, which connects to diverse information systems like email, file shares, groupware, instant messaging platforms, and file servers can be effective in monitoring more compliant data privacy protection measures. Using natural language processing to identify sensitive information named entities (like dates of birth, social security numbers, contact details, etc.), the .discover product is an essential part of monitoring the data privacy protection landscape.



### **Address Operational Disclosures**

The reality of an increasing number of workers accessing their IT systems (both customer premise and cloud-based) from outside the corporate network means that identifying rogue information assets that may be stored in under-managed applications is more critical than ever.



The increased exposure to malware and phishing that accompanies remote workers is yet another reason to reduce the “surface area” of exposed data that may be the target of a hack.

As with recruiting and onboarding, investing in an Information Governance solution that can detect leakage of private employee data (as well as private customer data) anywhere in the enterprise. Tools like .discover can help monitor compliance associated with both onboarding and inadvertent operational disclosures and can help meet the obligations associated with the GDPR Data Protection Impact Assessment<sup>4</sup>.

The .discover product connects to email systems (along with virtually every other class of enterprise information system), and is adept at crawling email systems and looking for named entities like birthdate, SSNs, and other sensitive data to ensure that no such information being shared, even when the reasons for doing so are innocent.

## Benefits of a Securing Employee and Candidate PII




Protecting the privacy employee and job candidate data is not optional, it is a required cost of doing business – especially in today’s heightened privacy awareness environment. That said, it should not be seen solely as a cost. There are also significant benefits that come from organizations opting for more active posture in protecting employee and candidate personally

<sup>4</sup>. <https://gdpr.eu/data-protection-impact-assessment-template/>



identifiable information, including:

- Improved compliance with data privacy protection regulations like GDPR, CCPA, and others. This means reducing or even eliminating the risk of costly fines that come from running afoul of these mandates.
- Reduced risk of litigation that comes from a data breach or other unintended disclosure. Recent employee data loss events from organizations like Nordstrom[5], T-Mobile[6], Ordnance[7], and the Office of Personnel Management[8] demonstrate that the threat of employee data loss is real, and that often class action litigation on behalf of employees is the result.
- Improved levels of employee loyalty and retention thanks to the strong stewardship of their information by employers. Employees, particularly the strongest performers, have choices about where they work. Showing a diligent concern for their digital wellbeing is an excellent way to earn their trust, and help ensure their long-term commitment to the organization.

Just as real these primary benefits are secondary  benefits that include stronger brand, increased valuation (for public companies), and improved revenue performance. Customers choose organizations that take privacy seriously more often than they choose those that are simply more price competitive[9]. That behavior extends to companies whose trust is earned based on their careful handling of employee data, not just customer or prospect data.

To learn more about how employee data can be protected

5. <https://www.tripwire.com/state-of-security/latest-security-news/nordstrom-breach/>

6. <https://www.insurancebusinessmag.com/us/news/cyber/tmobile-says-security-breach-exposed-employee-and-customer-data-216216.aspx>

7. <https://www.infosecurity-magazine.com/news/ordnance-survey-breach-hits/>

8. [https://en.wikipedia.org/wiki/Office\\_of\\_Personnel\\_Management\\_data\\_breach](https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach)

9. <https://www.inc.com/rhett-power/trust-is-as-important-as-price-for-todays-consumer.html>

throughout the enterprise, we invite you to visit [nyxeia.com](https://nyxeia.com) to understand how employee data privacy protection can be part of an effective overall information governance strategy.

Want to know more about employee data privacy protection? Nyxeia can help!

**[Watch the Webinar: Data Privacy is for Everyone - Including Employees](#)**

**[Contact Us: Info@nyxeia.com](mailto:Info@nyxeia.com)**

## About Nyxeia

Nyxeia provides the industry's most innovative software to help organizations identify their sensitive and valuable information to be more informed, efficient, and compliant with privacy protection regulations. Nyxeia enjoys stable ownership that has for the last 30 years created a portfolio of innovative companies that have become leaders in their markets.

## Nyxeia Products



**[.discover](#)**



**[.policy](#)**



**[.preserve](#)**



**[.process](#)**

[nyxeia.com](https://nyxeia.com) | 1251 Avenue of the Americas, Suite 3F | New York, NY 10020 | +1 (303) 854-9890 | [Info@nyxeia.com](mailto:Info@nyxeia.com)