Checklist: Responding to Employee DSARs

PLG
Potomac Law

Use this checklist to identify responsive data categories and systems when responding to an employee DSAR, even if an exception may ultimately apply. Tailor categories based on the employer's data processing activities.

- ✓ Validate that the employee is the requestor.
- ✓ Confirm that personal data about the employee is being processed
- ✓ Identify purposes for which data is processed (e.g., administration of employment relationship, payroll processing, benefits administration, performance management, legal compliance)
- ✓ Check third parties with whom employee data has been shared (e.g., payroll providers, benefits administrators, background check vendors, agencies)
- ✓ Check retention periods for each data category, or criteria used to determine retention
- ✓ Consider multiple datasets in the review of data to respond to the DSAR:

    - Data not collected directly from the employee and identify relevant sources (e.g., references, background checks, prior employers, recruiters)
    - Information about any automated decision-making or profiling (e.g., AI-assisted resume screening, algorithmic performance scoring)
    - HRIS data, including applicant tracking systems (recruiting and hiring records), payroll and compensation systems, benefits administration platforms, time and attendance systems (including badge/access logs), learning management and training records, and performance management platforms
    - Personnel records
    - Grievance, complaint, and investigation files involving the employee
    - Termination documentation (if applicable)
    - Email (employee's mailbox and custodians likely to have correspondence about the employee, such as direct manager, HR partner, department head)
    - Instant messaging and collaboration platforms (Slack, Microsoft Teams, etc.)
    - Shared drives, SharePoint, and document management systems
    - If applicable, IT system logs (network access, VPN usage, login records)
    - Device management data (company-issued laptops, phones)
    - Productivity monitoring or surveillance tools (screenshots, keystroke logging, browser history)
    - CCTV or security camera footage (if identifiable)
    - GPS or location tracking data (for field employees or company vehicles)

Bonne Levine, Partner
blevine@potomaclaw.com

Lisa Zolidis, Partner
lzolidis@potomaclaw.com