Regulatory Law Alert
January 2026

by: Robert J. Munnelly, Jr.

National Data Privacy Day: 8 Tips for Employers to Protect Company and Employee Data

National Data Privacy Day (January 28) is a timely reminder for employers that cybersecurity and data privacy are not just IT priorities — they are also workplace, compliance and business continuity priorities. Employers routinely collect and store highly sensitive employee, applicant and independent contractor information, including Social Security numbers, payroll data, medical information, background records and banking information. A data breach can expose an organization to regulatory penalties, litigation, operational disruption, and reputational harm.

Employers should use this annual checkpoint to evaluate whether their data protection practices are keeping pace with evolving threats and legal obligations.

© 2026 Davis, Malm & D'Agostine, P.C. All rights reserved

1. Train Employees on Cyber Awareness

Employees remain the first line of defense. Regular training should cover phishing detection, password hygiene, secure remote work practices, and proper handling of confidential employee and customer information. The "bad actors" are getting better at infiltrating systems. Periodic refreshers and simulated phishing exercises reinforce good habits and reduce risk.

2. Limit Access to HR and Personnel Data

Authorized personnel should be the only ones with access to payroll systems, personnel files, benefits platforms, and medical information. Conduct periodic access audits and immediately revoke access when employees change roles or leave the organization.

3. Strengthen Authentication and Device Security

Strong passwords and multi-factor authentication (MFA) for HR systems, remote access, cloud platforms, and email accounts should be required. Implement endpoint protection for laptops and mobile devices, especially for remote and hybrid employees.

4. Keep Systems Patched and Upgraded

Unpatched systems are a common entry point for cyber incidents. Employers should ensure timely updates of operating systems, HR software, payroll platforms, and security tools to address known vulnerabilities.

5. Encrypt and Back Up Sensitive Workforce Data

Employee data should be encrypted both in transit and at rest. Maintain secure, routine backups and test restoration procedures so operations can be restored quickly after a cyber event or ransomware incident.

© 2026 Davis, Malm & D'Agostine, P.C. All rights reserved

6. Maintain Written Policies and an Incident Response Plan

Employers should have clear policies addressing information security, data privacy, acceptable technology use, remote work security, and incident reporting, usually codified in a written information security program. An incident response plan helps ensure the organization can act quickly to evaluate a potential compromise, identify potential breaches, meet legal notification requirements, preserve evidence, and coordinate internal and external communications.

7. Manage Vendor and Payroll Provider Risk

Many employers rely on third-party vendors for payroll, benefits administration, recruiting platforms, and IT services. Vendor contracts should (and in some states must) include data security standards, breach notification obligations, and audit rights. Employers should require vendors to periodically confirm they maintain appropriate safeguards and insurance coverage.

8. Stay Current on Privacy and Employment Law Requirements

State privacy laws, biometric data rules and employee data protection and health care information protection requirements continue to expand and evolve. Regularly reviewing compliance obligations related to employee and contractor data collection, retention, monitoring and breach notification is a good practice for any employer.

Conclusion

Cybersecurity and data privacy require ongoing attention, not one-time fixes placed in a file cabinet and forgotten. Employers that treat cybersecurity and data privacy as core workforce risk issues — not just IT concerns — are better positioned to prevent incidents, maintain compliance, and protect their employees and their business.

© 2026 Davis, Malm & D'Agostine, P.C. All rights reserved

CONTACT

If you have any questions about data security or information privacy laws or would like a confidential assessment of your security-related policies, please contact Rob Munnelly in our Data Security and Information Privacy Practice.

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Davis Malm. You should seek professional counsel before taking any action on this information.

© 2026 Davis, Malm & D'Agostine, P.C. All rights reserved