International Journal of Multidisciplinary Research and Growth Evaluation.

The Impact of GDPR on HRIS: Strategies for Secure Employee Data Management

Ilango Kessavane
Independent Researcher, USA

* Corresponding Author: **Ilango Kessavane**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 02
March-April 2025
Received: 03-03-2025
Accepted: 01-04-2025
Page No: 1848-1852

Abstract
The General Data Protection Regulation (GDPR) has significantly changed how organizations handle personal data. HR departments manage a vast amount of sensitive information, from contact details and bank accounts to health records and performance data. Human Resource Information Systems (HRIS) are at the center of this transformation.
Designed to store and manage employee data efficiently, HRIS platforms must meet strict compliance requirements. Starting from how data is collected and stored to how it is accessed and deleted, every step must align with GDPR principles. The stakes are high: non-compliance can lead to significant fines, reputational damage, and a breakdown of trust between employees and employers.
This white paper explores how GDPR has changed the game for HR teams and the technology they use. It breaks down the key regulations that affect HRIS, outlines the risks of non-compliance, and provides practical strategies for creating a secure, compliant, and future-ready HR data environment.
The objective of this paper is to help HR leaders, IT teams, and compliance professionals understand their responsibilities under GDPR and implement solutions that protect employee information while supporting efficient HR operations. Whether updating an existing system or choosing a new one, this white paper provides the guidance needed to move forward with confidence.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.2.1848-1852

Keywords: General Data Protection Regulation, Human Resource, Privacy Regulation, Data Protection, Employee Data, HR Data, Compliance

1. Introduction

In the past few decades, data privacy laws in the European Union have transformed dramatically. What began as general directives to protect consumer data has evolved into one of the world's most comprehensive privacy regulations, the General Data Protection Regulation (GDPR). GDPR reshaped how organizations collect, store, and use personal information, and it doesn't stop with customer data. It extends into internal operations, especially Human Resources.

At the heart of HR operations is the Human Resource Information System (HRIS). It manages everything from recruitment records and payroll data to employee performance and health-related documents. These systems have brought efficiency and centralization, but they've also introduced complex risks. HRIS platforms hold the employees' sensitive personal data, making them a prime area of focus for privacy compliance. For HR teams, GDPR is a legal checkbox that helps to earn trust. Employees expect their personal details to be handled with care. Whether it's processing job applications, managing leave records, or handling disciplinary actions, every touchpoint must meet GDPR's standards for transparency, security, and fairness.

This white paper explores how GDPR affects HRIS and how companies can align their systems and practices. As regulations continue to evolve, the role of HR in protecting employee data is becoming very critical.

Organizations that take this seriously will have no issues with compliance and quickly gain employee's trust.

2. What is GDPR and why it matters to HR

The General Data Protection Regulation (GDPR) law came into effect in 2018 across the European Union. It was designed to give people more control over their personal data. Though it is focused on customer and marketing data, it also has major implications for how companies manage employee information.

GDPR is based on a few key principles that every HR department must follow:

- **Lawfulness and Transparency**: Employees should know what data is being collected, why it's needed, and how it will be used. Consent must be clear and informed, not buried in paperwork
- **Purpose Limitation**: Data should only be used for specific reasons shared with the employee. If the data was collected for payroll, it shouldn't be reused for performance evaluation unless explicitly stated.
- **Data Minimization**: Only data necessary for a specific task should be collected. Gathering data more than what is required is not compliant.
- **Accuracy**: Employee records must be kept up to date.
- **Storage Limitation**: Data shouldn't be held longer than needed and clear retention policies are essential.
- **Integrity and Confidentiality**: Security measures should be in place to prevent unauthorized access or loss.
- **Accountability**: Organizations must be able to prove they're following these rules.

Under GDPR employee data is personal data. This includes names, addresses, job titles, bank details, and identification numbers. Special category data, such as health records, disability information, or trade union membership are more sensitive. It requires stricter handling and can only be processed under specific conditions, such as explicit consent or legal obligation.

Failing to follow these rules can damage employee trust. That's why HR's role in GDPR compliance is a legal responsibility, but putting it into practice is quite challenging.

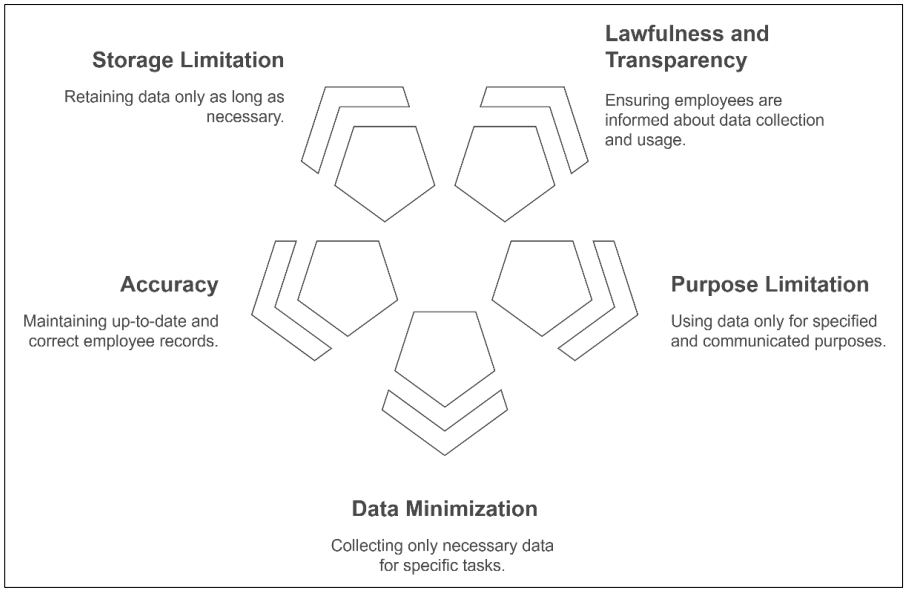

Fig 1: Navigating GDPR Complince in HR: Key Principles and Practices

3. The GDPR Challenges for HRIS

Human Resource Information Systems (HRIS) have become a central part of modern organizations. These platforms store everything, from hiring records and payroll data to performance reviews and sick leave reports. While this centralization brings efficiency, it also causes risks, especially in the context of the General Data Protection Regulation.

A centralized database has large volumes of sensitive employee data. That makes HRIS a prime target for cyberattacks and data breaches. If just one part of the system is compromised, a vast amount of personal information could be exposed. Under GDPR, this kind of breach doesn't require quick fixes. It demands transparency, mandatory reporting, and the possibility of significant fines.

Another challenge lies in legacy systems. Many organizations still rely on outdated HR software that wasn't designed with privacy in mind. These systems may lack basic features like access logs, role-based permissions, or automated data retention controls. Without built-in safeguards, it's hard for HR teams to track who accessed what data, when, and why.

Non-compliance with GDPR is a trust issue. A breach or violation can result in financial penalties of thousands to millions of euros. The impact on a company's reputation is even more damaging. Employees expect their personal information to be treated with care. If they feel that trust has been broken, it can affect morale and retention.

The stakes are even higher for multinational companies. These organizations operate across borders, and employee information may be stored or accessed in multiple countries. GDPR places strict rules on cross-border data transfers, especially when the data moves outside the EU. Without proper protection, these transfers can put a company at risk of non-compliance.

HRIS systems must protect the stored data. HR teams must move beyond convenience and functionality and ask a more critical question: is our HR technology helping us stay compliant, or putting us at risk? Answering this question is important because GDPR influences the way an organization handles its employee data.

4. GDPR Requirements for HRIS

HR departments handle vast amounts of employee data, from

job applications and payroll to performance evaluations and health-related absences. Under GDPR, every action involving this data must meet specific legal standards. For companies using an HRIS, understanding and applying the following GDPR requirements is essential.

4.1 Data collection

There must be a lawful method for collecting and processing employee information. This could include fulfilling a contract (like processing payroll), complying with legal obligations (like health and safety reporting), or legitimate interests (such as internal communication). GDPR views consent as valid only if it's freely given, which can be difficult in an employer-employee relationship, where power is not evenly balanced. Employers can't always fall back on consent as a safety net.

4.2 Control over data

One of the most important aspects of GDPR is it gives individuals more control over their data. Employees have the right to access their data, correct errors, restrict processing, and even request deletion in some cases. HRIS platforms must be able to support and respond to these requests quickly.

4.3 Data portability

Data portability allows employees to request a copy of their data in a readable format. It'll be useful when they change jobs. In certain HR scenarios, like recruitment or promotions, employees must be informed of automated decision-making (such as resume screening by AI). If used, there must be an option to request human review.

4.4 Data retention

GDPR demands that personal data be kept only when needed. HR teams must set clear retention periods for CVs, disciplinary records, or medical reports, and justify them if questioned.

Meeting these requirements means building transparency, respecting employee rights, and creating systems that protect privacy from the ground up. A well-designed HRIS can help companies stay compliant if set up with these GDPR requirements in mind.

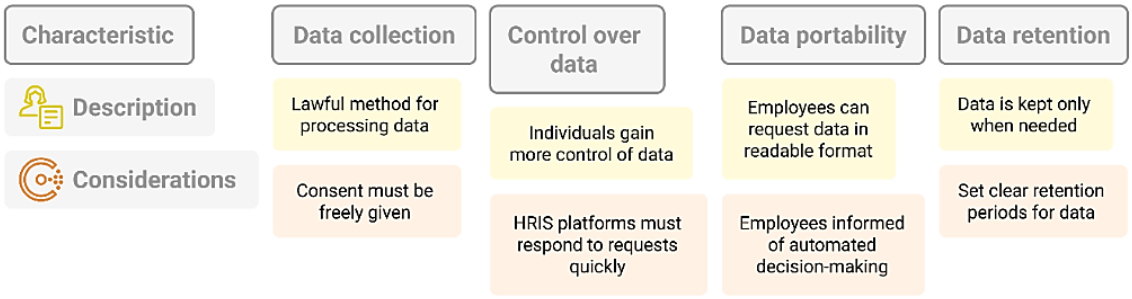

Fig 2: GDPR Requirements for HRIS

5. Strategies for GDPR-compliant employee data management

To protect employee privacy and stay compliant with GDPR, organizations must rethink how they manage data across their HR systems. Here are seven practical strategies to help HR teams align their HRIS with GDPR requirements.

5.1 Conducting a GDPR impact assessment (DPIA) for HRIS

Companies should run a Data Protection Impact Assessment before introducing or upgrading an HRIS. A DPIA helps identify privacy risks tied to personal data and ensures safeguards are in place before any system goes live. It's a proactive way to avoid problems later.

5.2 Embedding privacy by design and default in HR software

Privacy shouldn't be an afterthought. Human resource systems should be designed to collect only the necessary data, limit access, and protect information throughout its lifecycle. "Privacy by default" means settings are strict from day one, and employees don't have to opt into stronger protections because they're already in place.

5.3 Updating employee data collection and consent mechanisms

Forms, portals, and onboarding systems must clearly explain what data is being collected and why. Consent should be sought only when it's truly voluntary and necessary. For other use cases, HR should rely on lawful bases such as employment contracts or legal obligations.

5.4 Strengthening access controls and role-based permissions

Not every HR staff member needs access to all employee information. Role-based access ensures people see only the information relevant to their job. It also helps prevent accidental exposure and limits internal risks.

5.5 Data encryption and secure storage protocols

Data should be encrypted both at rest and in transit. Whether information is stored on-premise or in the cloud, strong encryption and secure storage practices protect against unauthorized access and data breaches.

5.6 Regular audit trails and activity logging in HRIS

HRIS platforms should track who accessed or modified employee data and when. These audit trails provide transparency, support internal investigations, and help demonstrate compliance during regulatory reviews.

5.7 Data retention and deletion workflows

Companies should clearly decide how long they will keep different types of HR data, such as applications, contracts, or disciplinary records. Automated workflows that archive or delete data reduce risk and support GDPR's storage limitation principle.

These strategies form the foundation of secure, compliant, and employee-friendly HR data management.

6. Integrating HR, legal, and IT teams

Managing employee information securely requires close collaboration between HR, legal, and IT departments. Each department offers a unique perspective and the result is stronger data protection across the board.

A great starting point is to create a cross-functional GDPR task force. This group should include representatives from HR, IT, and legal and meet regularly to review policies, address concerns, and adapt to regulatory updates. The HR team understands what data is collected and why, the legal team ensures it's done in line with GDPR, and the IT team takes care of the systems and security that support it all.

It's essential to build internal awareness and training for HR staff. HR teams work with sensitive data daily, but everyone may not be aware of the finer points of GDPR, like when consent is needed, how long data can be kept, or what to do in case of a breach. Scenario-based training can go a long way in helping staff understand their responsibilities and avoid costly mistakes.

Companies that regularly handle large volumes of data should consider appointing a Data Protection Officer (DPO). This is a strategic move. A DPO acts as the bridge between departments, keeps up with changing regulations, and ensures the organization thinks about privacy. In some cases, a DPO may be legally required.

By building a strong connection between HR, legal, and IT, companies can create a culture of accountability and care around employee information. In a world where privacy is increasingly valued, that's a competitive advantage worth investing in.

7. Choosing your HRIS vendor

Since your HR software will handle sensitive personal data, you need a vendor that takes GDPR seriously. A few key steps can help you make the right choice.

Start with a GDPR-readiness checklist. A reliable HRIS vendor should be able to show how they comply with GDPR. This includes data encryption, access controls, audit trails, data retention settings, and tools that support employee rights like data access and deletion. Ask for documentation that outlines privacy policies and technical safeguards.

When evaluating potential vendors, ask the right questions.

- Where is the data stored?
- What measures are in place to prevent unauthorized access?
- Can the system support "right to be forgotten" requests?
- What happens to employee data if the contract ends?

Look closely at Service-Level Agreements (SLAs) and Data Processing Addendums (DPAs). These legal documents set clear expectations around how data is handled, who is responsible for what, and what happens during a data breach. A strong DPA should cover how the vendor will process data and ensure they don't use it for any purpose the organization hasn't agreed to.

Choosing a vendor that meets GDPR standards is a long-term investment in protecting employees' privacy and the company's reputation. The right HRIS partner will deliver great tools and share the company's commitment to keeping data safe and compliant.

8. Maintaining compliance through continuous adaptation

GDPR compliance is an ongoing process. Data privacy regulations continue to evolve, and so do the ways organizations follow to collect, store, and use employee information. Businesses must build regular checkpoints to assess, improve, and adapt. They can't afford to become complacent. New laws are emerging, and some may overlap with or extend GDPR principles. HR teams must stay alert, working with legal and compliance teams to interpret these changes and understand their impact on HR practices.

Equally important is monitoring changes in how data is processed. Whether adopting a new recruitment tool, expanding remote work, or launching internal employee wellness programs, any new use of data should be evaluated for risks. Changes can introduce gaps in privacy protection if not reviewed properly. Quarterly or biannual audits ensure your system supports current GDPR requirements. These reviews make sure your system evolves with your policies.

Even the best software can't protect against human error. Make training a part of your company culture. Ongoing training for HR staff and system administrators can keep teams informed and accountable. One powerful way to support this continuous approach is by leveraging automation. Use your HRIS to schedule automatic data deletion, send alerts when records are due for review, or flag access anomalies.

Automation doesn't replace human oversight, but it does make it easier to stay audit-ready and responsive. When a compliance check or employee request comes in, you're prepared, not scrambling.

GDPR compliance is about building habits that protect employee trust and help your organization stay ahead. A flexible, forward-thinking approach ensures your HRIS keeps pace with the future of privacy.

9. The road ahead

As data privacy continues to gain attention, organizations must prepare for regulations like GDPR. Laws such as the EU AI Act and state-level privacy regulations are set to reshape how personal data is collected and used, in areas like automated decision-making and AI-driven HR tools. Being proactive can save companies from bigger changes and risks later.

One of the best ways to prepare is by keeping HR systems flexible. Your HRIS should be able to adjust to new rules, whether updating consent forms, adding audit features, or refining data retention settings. Work closely with your HR tech vendors to ensure your tools can scale with legal demands.

Success lies in building a culture of privacy. Create an environment where everyone understands the importance of protecting personal data and respecting the people behind the data.

That brings us to a crucial mindset shift: ethical data handling. Legal compliance sets the minimum bar, but responsible organizations go further. They ask, "Just because we can collect this data, should we?" Being thoughtful about what data is collected, how long it's kept, and who has access shows employees that their privacy matters.

Looking ahead, HR leaders who combine smart tools, flexible systems, and ethical practices will stay compliant and earn long-term trust from their workforce. Those who treat

data with care today are best positioned for tomorrow.

10. Closing the Loop

Navigating GDPR in the context of HRIS is no small task, but it's essential. Businesses must take clear, practical steps to ensure they're compliant and respectful of their employees' right to privacy. This includes reviewing how data is collected, processed, stored, and deleted. Companies should conduct regular data protection impact assessments, strengthen access controls, keep consent mechanisms updated, and ensure their HR software is built with privacy in mind.

Choosing a GDPR-ready HRIS vendor and offering continuous training to staff helps in creating a strong foundation for compliance. Companies that prioritize privacy earn trust from their employees, reduce the risk of costly data breaches, and are better prepared for future regulations. They will be the ones leading the way in the years ahead.

11. References

1. https://www.researchgate.net/publication/358194487_The_relationship_between_human_resources_activities_and_the_general_data_protection_regulation International Conference on Business Excellence, Dec 2021
2. https://www.researchgate.net/publication/376134134_Safeguarding_Employee_Data_A_Comprehensive_Guide_to_Ensuring_Data_Privacy_in_HR_Technologies International Journal of Computer Techniques, Nov 2023
3. https://www.researchgate.net/publication/348391095_HUMAN_RESOURCES_AND_PERSONAL_DATA_PROTECTION_AN_INDISSOLUBLE_RELATIONSHIP Journal of Public Administration Finance and Law, Jan 2021
4. https://www.researchgate.net/publication/382073552_The_Influence_of_Cybersecurity_on_Human_Resources_Legal_Practices_and_Ethical_Standards July 2024
5. https://www.researchgate.net/publication/384627963_Data_Privacy_and_Security_Strengthening_data_privacy_and_security_measures_to_protect_sensitive_employee_information Oct 2024
6. https://www.researchgate.net/publication/387224965_Ensuring_Compliance_with_GDPR_CCPA_and_Other_Data_Protection_Regulations_Challenges_and_Best_Practices May 2023