Workday Ruling: How Europe's Top Courts Raised the Bar for Employee Data Protection

Insights
7.23.25

Cloud-based HR systems have become standard for multinational businesses, driving efficiency but also increasing compliance and privacy risks. Indeed, a recent Workday case, which originated in Germany, has clarified the limits of collective labor agreements and set important General Data Protection Regulation (GDPR) benchmarks for employee data processing. Read on to learn about the key legal findings and their significance for US employers with operations in Europe.

Key Takeaways:

The Workday case – which was taken to the Court of Justice of the European Union (CJEU) – resulted in a new standard for European workplace privacy. It confirms:

- Even minor breaches, like over-inclusion of personal data in a temporary software test, may result in compensation claims.
- No collective agreement can dilute GDPR protections.
- All intra-group data transfers, especially those involving cloud tools or real test data, are subject to stringent, reviewable limits.
- Compensable damage does not require financial loss. Rather, a loss of control over personal data suffices.

The Workday Case Details

A German employer within an international group sought to introduce the Workday cloud HR platform in 2017. The company's works council (*Betriebsrat*), which is a representative body for a company's employees representing the employees, approved a collective agreement (*Betriebsvereinbarung*) permitting temporary use of specified categories of employee data, like name, entry date, and work location during a pilot phase to "feed" the system. Despite these limits, the company transferred additional sensitive data for testing, including salary details, private address, birth date, marital status, social security, and tax ID.

In consequence, an employee claimed immaterial damages under Article 82 GDPR for the unlawful transfer, claiming loss of control over his personal data. Lower courts dismissed his claim, but the

Federal Labor Court (*Bundesarbeitsgericht, BAG*) ultimately referred some questions of EU law to the CJEU, before partly siding with the employee.

The BAG paused its review and presented the CJEU with questions regarding:

- whether a *Betriebsvereinbarung* could justify data transfers inconsistent with stricter GDPR rules;
- the standard for nonmaterial damages under Article 82 GDPR; and
- the extent of national courts' review over such agreements.

CJEU Findings and European Standards

- The CJEU held that **no collective agreement could bypass GDPR standards**. All such collective agreements must:
  - Strictly adhere to GDPR's principles of necessity, proportionality, data minimization, purpose limitation, and storage limitation.
  - Be subject to full judicial review: courts must substantively verify that each aspect of the agreement and any data processing it permits are strictly GDPR-compliant.
  - Not authorize any processing that would be unlawful under the GDPR, regardless of declarations or intentions in the agreement.

The BAG's Final Ruling: Key Takeaways

- **Breach Confirmed:** Transferring employee data categories beyond those in the works agreement – without an independent legal basis – violated GDPR.
- **Immaterial Damage and Loss of Control:** The BAG recognized that the mere loss of control over personal data constitutes a compensable nonmaterial damage. A claimant does not need to prove economic loss or a certain threshold of seriousness.
- **Employers' Due Diligence:** The decision restates the need for GDPR-compliance in every step of HR data handling: policy, collective agreements, system architecture, and actual data transfer.

Harmonized Protection: No "National Flexibilities"

- The CJEU underscored that the GDPR sets a *minimum, harmonized standard* for personal data protection across the EU.
- Member States and social partners, through works councils or collective agreements, may not lower these standards.

5 Key Takeaways for Employers

- **Collective Agreements:** When using a collective agreement to justify processing employee data, ensure every detail aligns with the GDPR, with a substantiated, lawful basis for each data transfer.
- **Testing and Real Data:** Using real employee data for system testing is only permissible if strictly necessary, and only the data expressly allowed should be transferred.
- **Documentation:** Employers should clearly document and justify why data is processed or transferred and be prepared for judicial scrutiny.
- **Compliance and Training:** HR, legal, and IT should work together to ensure internal policies, collective agreements, and practices withstand potential court challenges.
- **Minimizing Overreach:** The threshold for immaterial damages is low: loss of control alone is compensable. So, employees are now better positioned to assert GDPR claims, and employers have an incentive to minimize overreaching or accidental misuse.

Conclusion

We will continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our International Practice Group or our Privacy and Cyber team.

Related People

Mauricio Foeth
Of Counsel
+52 55 48992148/+49 1575 8880464
Email

Service Focus

International

Privacy and Cyber