OXFORD COLLEGE SCIENTIFIC JOURNAL
Volume 1, Issue 3 (2026) · Open access

REVIEW ARTICLE · LAW

People Analytics and Data Protection: Applying GDPR Principles to Human Resources Data

Oxford College Research Office
Oxford College, London, United Kingdom

Published 24 November 2026 · Volume 1, Issue 3 (2026)

ABSTRACT

Organisations increasingly analyse workforce data to inform recruitment, performance management, retention and workforce planning. This "people analytics" can improve decisions, but it also processes personal data about individuals in a relationship marked by an imbalance of power. This review applies the principles of the European Union's General Data Protection Regulation (GDPR) to human resources analytics: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. It discusses the limited role of consent in employment, the special categories of personal data, rights relating to automated decision-making, and the role of data protection impact assessments. It also notes that the European Union's Artificial Intelligence Act treats many AI systems used in employment as high-risk. The article proposes a set of practical safeguards and concludes that responsible people analytics depends on proportionality, transparency and meaningful human involvement.

Keywords: people analytics; HR analytics; GDPR; data protection; employee privacy; automated decision-making; AI Act

1. Introduction

Human resources functions hold extensive information about employees and candidates: contact details, qualifications, performance reviews, absence records, pay, training and, increasingly, digital traces from workplace systems. "People analytics" uses this information to identify patterns — for example the factors associated with turnover or the effectiveness of training programmes — and to support decisions.

The same data, however, relate to identifiable individuals who depend on their employer for their livelihood. This review examines how data protection law, using the European Union's General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") as the reference framework, applies to people analytics, and proposes practical safeguards. It is an overview of principles and not legal advice.

2. The employment context

The relationship between employer and employee is characterised by an imbalance of power. European data protection authorities, in Opinion 2/2017 on data processing at work (Article 29 Working Party, 2017), emphasised that employees are seldom in a position to give, refuse or withdraw consent freely, and that the increasing ability of technology to monitor and analyse behav-

iour requires particular care. As a result, consent is rarely an appropriate legal basis for processing employee data, except in situations where refusing has no adverse consequences.

3. The GDPR principles applied

Article 5 GDPR sets out the principles that govern all processing of personal data.

3.1 Lawfulness, fairness and transparency

Processing requires a legal basis under Article 6 — in employment typically the performance of the employment contract, compliance with a legal obligation or the employer's legitimate interests, subject to a balancing test. Fairness requires that analytics does not produce unexpected or unjustified effects for employees. Transparency requires clear information about what data are used, for what purposes and with what consequences.

3.2 Purpose limitation

Data collected for one purpose — for example processing payroll — should not be reused for an incompatible purpose, such as predicting which employees may resign, without assessment and, where necessary, a new legal basis and information to employees.

3.3 Data minimisation

Only data that are adequate, relevant and limited to what is necessary should be used. Analytics projects tend to favour "more data"; data protection requires the opposite question: what is the minimum needed to answer this question? Aggregated or pseudonymised data are often sufficient for workforce-level insights.

3.4 Accuracy

Inaccurate or outdated records lead to wrong conclusions about individuals. Analytics should include checks on data quality and allow employees to correct errors.

3.5 Storage limitation

Data should be kept no longer than necessary. Historical datasets retained "for future analysis" without a defined purpose are difficult to justify.

3.6 Integrity and confidentiality

HR data are sensitive and must be protected by appropriate security measures, including access controls that limit who can see individual-level results.

3.7 Accountability

The employer must be able to demonstrate compliance — through records of processing, documented assessments and policies.

4. Special categories of data

Article 9 GDPR restricts the processing of special categories of personal data, including data concerning health, racial or ethnic origin, religious beliefs, trade-union membership and biometric data used for identification. HR data often include health information (for example absence reasons) and may be used for equality monitoring. Such processing requires a specific condition under Article 9 and strong safeguards; inferring special-category information from other data also raises serious concerns.

5. Automated decision-making

Article 22 GDPR gives individuals the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them, subject to limited exceptions and safeguards such as the right to obtain human intervention. Decisions on recruitment, promotion or dismissal can have such effects. Human involvement must be meaningful: a reviewer who routinely accepts the system's recommendation without independent assessment does not change the nature of the decision.

6. Impact assessments and the AI Act

Article 35 GDPR requires a data protection impact assessment (DPIA) where processing is likely to result in a high risk to individuals' rights and freedoms. Systematic evaluation of employees and large-scale monitoring commonly meet this threshold. A DPIA describes the processing, assesses necessity and proportionality, identifies risks and sets out mitigating measures.

The European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) additionally classifies as high-risk many AI systems intended to be used in employment — including for recruitment and selection and for decisions affecting work relationships, such as promotion, termination, task allocation and performance monitoring. Such systems are subject to requirements on risk management, data governance, transparency and human oversight.

7. Practical safeguards

1. Define a clear and legitimate question before collecting or combining data.
2. Prefer aggregated and pseudonymised analysis for workforce-level insights.
3. Conduct a DPIA for analytics that evaluates individuals or monitors behaviour.
4. Inform employees clearly, and consult employee representatives where applicable.
5. Exclude or strictly control special-category data and avoid inferring it.
6. Ensure meaningful human review of decisions affecting individuals.
7. Test models for bias and monitor outcomes for different groups.
8. Restrict access to individual-level results and set retention periods.

8. Conclusion

People analytics can help organisations make better and fairer workforce decisions, but only if it respects the rights of the people whose data it uses. Applying the GDPR principles — especially purpose limitation, minimisation and transparency — together with impact assessments and meaningful human involvement, allows organisations to gain insight while maintaining trust.

References

Article 29 Data Protection Working Party. (2017). *Opinion 2/2017 on data processing at work* (WP 249). European Commission.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union,* L 119.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.*

Article information. This review article was prepared by the Oxford College Research Office with the assistance of generative AI tools, and was reviewed and approved by the editorial office of the Oxford College Scientific Journal. It synthesises published literature and does not report new empirical data.

How to cite. Oxford College Research Office (2026). People Analytics and Data Protection: Applying GDPR Principles to Human Resources Data. *Oxford College Scientific Journal*, 1(3).

Licence. © 2026 Oxford College. Published open access by Oxford College.