Compare the rules of the GDPR - in particular, with relation to the securing of personal data rule, with either similar compliance laws within your country of residence, or with the ICO in the UK

The lucrative value of personal data in the current digital economy necessitates robust legal frameworks to prevent its misuse. In the United Kingdom (UK), the primary authority overseeing this landscape is the Information Commissioner's Office (ICO), which enforces both the Data Protection Act 2018 and the UK GDPR.

Securing Personal Data

Under Article 5(1)(f) of the GDPR, the principle of 'integrity and confidentiality' is paramount. It requires data controllers to implement "appropriate technical and organisational measures" to protect data against unauthorised processing or accidental loss.

While the GDPR provides the high-level legal requirement, the ICO offers the granular interpretation for UK businesses. For example, the ICO provides specific checklists on encryption and cyber security that translate the broad EU principles into actionable compliance for British SMEs.

Comparative Analysis: GDPR vs. ICO Guidance

The relationship between the EU and UK frameworks is symbiotic rather than contradictory. The EU GDPR is overseen by the European Data Protection Board (EDPB) and requires multi-state cooperation for cross-border issues, whereas the UK GDPR is an independent regime enforced solely by the ICO post-Brexit. While both maintain identical core principles, such as data minimisation and purpose limitation, the ICO differentiates itself through detailed outcome-based guidance tailored to the British industrial strategy. Recent guidance from the ICO on anonymisation allows for a risk-based approach, as opposed to the stricter, absolute standards often favoured by the EDPB (Stevens & Bolton LLP, 2025).

Case Study: British Airways

The ICO intended to fine British Airways over £183 million after a 2018 cyber-attack compromised the data of roughly 400,000 customers. The regulator highlighted that BA had failed to implement basic security measures required by Article 32 of the GDPR, such as multi-factor authentication (MFA) and the encryption of administrator login credentials (ICO, 2020). Although the fine was eventually reduced to £20 million due to the economic impact of the pandemic and BA's prompt remedial actions, the case solidified the ICO's authority to issue multi-million-pound penalties for 'security-by-design' failures.

References

Information Commissioner's Office (ICO) (2020) *ICO fines British Airways £20m for data breach affecting more than 400,000 customers*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach/ (Accessed: 16 January 2026).

Jay, R. (2021) *Data protection: law and practice*. 6th edn. London: Sweet & Maxwell.

Kunstein, M. (2022) 'The UK's data protection regime after Brexit: adequacy and the future of data flows', *International Review of Law, Computers & Technology*, 36(2), pp. 145–163. doi: 10.1080/13600869.2022.2045672.

Stevens & Bolton LLP (2025) *ICO and EDPB: anonymisation and pseudonymisation - safeguarding personal data*. Available at: https://www.stevens-bolton.com/site/insights/articles/ico-and-edpb-anonymisation-and-pseudonymisation (Accessed: 16 January 2026).