Collaborative Discussion 2 - Comparing Compliance Laws

Discussion Topic

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 ICO refers to this rule as '**Security**' and you should discuss your findings in relation to the standards set out and the exemptions that exist:

- 'The securing personal data principle of the GDPR: Personal data shall be processed in a manner that ensures appropriate security of the personal data...' (**ICO.org.uk**).

Instructions

- Go to the discussion forum and create an initial post of your contribution to the discussion.
- Review the Lecturecast and reading for this Unit.
- Review other literature in conjunction with this paper to enhance your post.
- Demonstrate that you understand the topic covered and ensure you use references to academic literature (journals, books, reports, etc.).

Learning Outcomes

- Identify and manage challenges, security issues and risks, limitations, and opportunities in data wrangling.

Initial Post

by Valentina Mercieca - Friday, 13 December 2024, 3:56 PM

Number of replies: 0

While the GDPR and the UK GDPR share foundational principles, including the need to implement appropriate security measures for personal data, there are subtle differences in how these rules are applied and enforced by the ICO. The GDPR, as an EU regulation, establishes broad principles that member states must follow, while the ICO has tailored its interpretation of the UK GDPR to the specific legal and operational context of the United Kingdom. These differences are evident in areas such as enforcement, exemptions, and practical guidance.

Both the GDPR and UK GDPR require organisations to implement appropriate technical and organisational measures to ensure the security of personal data, as outlined in Article 32 of the GDPR and its UK counterpart. These measures include encryption, pseudonymisation, access controls, regular testing of systems, and ensuring the ongoing confidentiality, integrity, and availability of data. While the EU GDPR's security principles are consistently applied across member states, the ICO adopts a more tailored, risk-based approach for the UK. This approach encourages organisations to implement security measures proportionate to the sensitivity of the data and associated risks.

The ICO provides detailed guidance to help businesses meet these requirements, particularly for small and medium-sized enterprises (SMEs). For example, the ICO's "Advice for Small Organisations" simplifies compliance for smaller businesses by offering practical examples and tools for safeguarding data (ICO, N.D.).

Enforcement under the EU GDPR is managed by individual Data Protection Authorities (DPAs) in each member state, coordinated by the EDPB to ensure consistency. This collective oversight often results in stricter enforcement across the EU, particularly in cases involving multinational corporations. For example, France's CNIL imposed a €50 million fine on Google in 2019 for insufficient transparency and lack of valid consent for personalised advertising (EDPB, 2019).

By contrast, the ICO operates independently post-Brexit, granting it greater flexibility in enforcing the UK GDPR. While the ICO retains the authority to issue significant fines—up to £17.5 million or 4% of global annual turnover—it often demonstrates a pragmatic and collaborative approach. For instance, the ICO initially proposed a £183 million fine against British Airways in 2019 for a major data breach but later reduced it to £20 million in recognition of the financial pressures faced by the airline during the COVID-19 pandemic (Page, 2020). This decision highlights the ICO's focus on balancing enforcement with economic realities, offering businesses a degree of leniency in exceptional circumstances.

The EU GDPR provides exemptions for specific scenarios, such as processing data in the public interest or for journalistic purposes, which are applied uniformly across member states with limited derogations allowed. In contrast, the UK GDPR, supplemented by the Data Protection Act 2018, includes exemptions tailored to UK-specific contexts. These exemptions (ICO, N.D.) address areas such as national security, crime prevention, and tax purposes and are often broader than those allowed under the EU GDPR. This reflects the UK's legislative priorities and its focus on domestic needs.

For organisations operating in both the UK and EU, navigating the nuanced differences between the GDPR and UK GDPR presents compliance challenges. For instance, data breaches must be

reported within 72 hours under both frameworks, but the interpretation of what constitutes a "risk to data subjects" can vary. The ICO's emphasis on proportionality and risk-based decision-making may provide more flexibility for UK businesses, particularly SMEs, but it also introduces potential inconsistencies compared to the stricter enforcement seen in some EU member states.

References

EDPB. (2019). The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC. Available from: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en [Accessed 13 December 2024].

ICO. (N.D.). A Guide to the Data Protection Exemptions. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/ [Accessed 13 December 2024].

ICO. (N.D.). Advice for Small Organisations. Available from: https://ico.org.uk/for-organisations/advice-for-small-organisations/ [Accessed 13 December 2024].

Page, C. (2020). U.K. Privacy Watchdog Hits British Airways with Record-Breaking £20 Million GDPR Fine. Available from: https://www.forbes.com/sites/carlypage/2020/10/16/ico-hits-british-airways-with-record-breaking-fine-for-2018-data-breach/ [Accessed 13 December 2024].