DBD: Collaborative Discussion 2 - Comparing Compliance Laws

Initial Post

The GDPR requires that all personal data conforms to measures to ensure the correct level of security this may include: the pseudonymisation and encryption of personal data, ongoing assessment of security measures etc (GDPR Art. 32, 2016). The ICO expands on the GDPR providing information more specific to the UK that is also in conjunction with the data protection act (DPA) 2018. Within the security section of the ICO guidelines the 'CIA triad' (confidentiality, integrity and availability) is highlighted as the three key elements of data security. If any of these key elements are compromised then data will be at risk (ICO- Security, nd).

In particular situations the DPA can grant exemptions from certain GDPR provisions (ICO, nd). While both the GDPR and ICO deem that data security is at the highest importance, the guidelines allow for organisations to balance data security with the principle of proportionality. Proportionality allows companies to avoid implementing excessive security measures that have the potential to severely hinder the necessary processing of data. In order for the exemption to be granted it must be in line with the accountability principle. Justification for the exemption must be documented to demonstrate compliance (Mourby et al., 2019). Each consideration for exemption is reviewed on a case-by-case basis, if no exemption is identified the GDPR must be enforced (ICO, nd).

GDPR Art. 32 – security of processing (2016) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-32-gdpr/ (Accessed: 21 June 2023).

ICO. (nd) 'A guide to the data protection exemptions'. ICO. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/ (Accessed: 21 June 2023).

ICO- *Security*. (nd) *A guide to data security*, *ICO- Security*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/#2 (Accessed: 23 June 2023).

Mourby, M. *et al.* (2019) 'Governance of Academic Research Data under the GDPR—lessons from the UK', *International Data Privacy Law*, 9(3), pp. 192–206. doi:10.1093/idpl/ipz010.

Response from Giuseppe

by Giuseppe Raneli - Wednesday, 28 June 2023, 2:37 PM

Hi Shaun,

Your post highlights some similarities and convergences between both frameworks, and ultimately, GDPR and the UK's ICO guidelines within the Data Protection Act (DPA) 2018 framework both stress strong data protection measures. They share the application of the 'CIA triad', which stands for confidentiality, integrity, and availability, to safeguard data. However, as you rightly pointed out, a significant differentiation emerges in how they handle the practical implementation of data security measures.

The DPA 2018 demonstrates flexibility by offering the possibility for exemptions from specific GDPR provisions in line with the principle of proportionality. This principle suggests that while data security is paramount, it should not impose unnecessarily rigid or excessive measures that could obstruct critical data processing activities (Georgiadis and Poels,2022).

However, exemptions are not unregulated. To ensure that the intent of data protection is not compromised, the principle of accountability stipulates that exemptions must be well-documented, justified, and demonstrate compliance with broader data protection objectives. This process demonstrates the commitment of the ICO/DPA to strike a balance between ensuring data security and avoiding hindrances to necessary data processing activities.

In conclusion, while GDPR and the ICO/DPA stress the importance of stringent data security, their approach to flexibility and proportionality differ. The ICO/DPA guidelines reflect the nuanced needs of different contexts and uphold the core principles of data protection, demonstrating the importance of a balanced, pragmatic approach in implementing data security measures.

References:

Georgiadis, G.,and Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. Computer Law & Security Review, 44, 105640.

Summary Post

As a result of responses from my peers I have been able to refine my initial post. There are many similarities and differences between the GDPR and ICO/DPA. The GDPR requires that all personal data conforms to measures to ensure the correct level of security this may include: the pseudonymisation and encryption of personal data, ongoing assessment of security measures etc (GDPR Art. 32, 2016). The ICO expands on the GDPR providing information more specific to the UK that is also in conjunction with the data protection act (DPA) 2018. Within the security section of the ICO guidelines the 'CIA triad' (confidentiality, integrity and availability) is highlighted as the three key elements of data security. If any of these key elements are compromised then data will be at risk (ICO- Security, nd).

The DPO (2018) identifies that the ICO/DPA offers a wider scope than the GDPR in a number of factors including: criminal sanctions and fines for infringements, processes relating to aspects outside of the scope of EU law. The GDPR is governed by the Court of Justice of the European Union (CJEU), once the UK leaves the EU the DPA will be solely governed by the UK justice system (Dpo, 2018).

In particular situations the DPA can grant exemptions from certain GDPR provisions (ICO, nd). While both the GDPR and ICO deem that data security is at the highest importance, the guidelines allow for organisations to balance data security with the principle of proportionality. Proportionality allows companies to avoid implementing excessive security measures that have the potential to severely hinder the necessary processing of data. In order for the exemption to be granted it must be in line with the accountability principle. Justification for the exemption must be documented to demonstrate compliance (Mourby et al., 2019). Each consideration for exemption is reviewed on a case-by-case basis, if no exemption is identified the GDPR must be enforced (ICO, nd).

Dpo (2018) *What is the difference between the DPA 2018 and the GDPR?*, *Outsourced Data Protection Officers GDPR and Data Protection Compliance*. Available at: https://www.dpocentre.com/difference-dpa-2018-and-gdpr/ (Accessed: 11 July 2023).

GDPR Art. 32 – security of processing (2016) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-32-gdpr/ (Accessed: 21 June 2023).

ICO. (nd) 'A guide to the data protection exemptions'. ICO. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/ (Accessed: 21 June 2023).

ICO- *Security*. (nd) *A guide to data security*, *ICO- Security*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/#2 (Accessed: 23 June 2023).

Mourby, M. *et al.* (2019) 'Governance of Academic Research Data under the GDPR—lessons from the UK', *International Data Privacy Law*, 9(3), pp. 192–206. doi:10.1093/idpl/ipz010.