Collaborative Discussion 2:

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**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/)).

The General Data Protection Regulation (GDPR) mandates that personal data must be processed in a manner that ensures "appropriate security" to protect against risks such as unauthorized access, data breaches, or loss (ICO, n.d.). This principle emphasizes measures like encryption, pseudonymization, and access control to safeguard sensitive information.

In the United States, there is no single, comprehensive data protection law equivalent to the GDPR. Instead, U.S. compliance is sector-specific, with regulations like the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Gramm-Leach-Bliley Act (GLBA) for financial institutions. Both require organizations to implement reasonable security measures but lack the GDPR's broad, unified approach. For example, HIPAA’s Security Rule mandates administrative, physical, and technical safeguards for electronic Protected Health Information (ePHI) (HHS, 2022). These measures align with GDPR’s requirements for ensuring data confidentiality, integrity, and availability.

However, significant differences exist. GDPR applies to all entities processing data of EU citizens, whereas U.S. laws are often narrower in scope. Additionally, the GDPR emphasizes accountability, requiring organizations to document security measures, conduct Data Protection Impact Assessments (DPIAs), and appoint a Data Protection Officer (DPO) in certain cases (EU GDPR, 2016). In contrast, U.S. laws do not universally require such roles or processes.

Both frameworks recognize exemptions. For instance, GDPR exempts processing done solely for personal or household purposes, while HIPAA exempts de-identified data from strict security requirements (ICO, n.d.; HHS, 2022). The GDPR sets a higher bar for enforcement, with fines reaching 20 million euros or 4% of global revenue, compared to smaller penalties under HIPAA (EU GDPR, 2016).

Ultimately, while both prioritize securing personal data, the GDPR's comprehensive nature contrasts with the U.S.’s fragmented approach.

**References**

* EU GDPR (2016) *General Data Protection Regulation (GDPR)*. Available at: <https://eur-lex.europa.eu> (Accessed: 27 January 2025).
* HHS (2022) *Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Available at: <https://www.hhs.gov> (Accessed: 27 January 2025).
* ICO (n.d.) *Security*. Available at: <https://ico.org.uk> (Accessed: 27 January 2025).
* FTC (n.d.) *Gramm-Leach-Bliley Act (GLBA)*. Available at: <https://www.ftc.gov> (Accessed: 27 January 2025).