Activity
Read the article by Barafort et al (2018) and the blog by Kirvan (2021). Review the websites listed in the blog and then answer the following questions:

Which of the frameworks do you think would be applicable to the following organisations:

- International bank
    - Assumptions :
        - As an international bank, it also does business in the EU.
        - The bank offers online payment services.
    - PCI-DSS
    - GDPR
    - Country specific frameworks in which the bank is running
- Large hospital.
    - Assumptions:
        - It is not a school medical center.
        - It provides medical treatment to the general public.
        - The hospital is based in the EU.
        - The hospital is also consuming data of US citizens
    - GDPR
    - HIPAA
    - PCI- SSC (If it is the US, as people pay with credit cards)
- Large food manufacturing factory.
    - Assumptions:
        - The factory is in the EU or serves customers there.
        - Uses automated machines.
        - The production facility is connected to the internet
    - GDPR
    - PCI- DSS

Recommendations

- A Data Protection Officer will be designated who is responsible for ensuring that the organization is providing the organization's compliance with GDPR (Regulation, G.D.P., 2018).
- Strictly apply §24(1). GDPR, where the organization considers the nature, scope, implement rights of the data subject and defines the purpose of the data processing (Akhlaghpour S et al., 2021, pg.201).
- Strictly apply §25(1) GDPR, where the organization implements all the necessary technical aspects to guarantee the rights provided by GDPR (Akhlaghpour S et al., 2021, pg.202).
- Carry out risk assessment analysis when new technologies or processes are added to the system.
- Conduct regular audits from internal and external agents to ensure compliance with the applied frameworks, i.e., GDPR, HIPAA, and PCII (Saeed, S, et.al, 2020, pg. 1460).

References

Akhlaghpour, S., Hassandoust, F., Fatehi, F., Burton-Jones, A. and Hynd, A., 2021. Learning from Enforcement Cases to Manage GDPR Risks. MIS Quarterly Executive, 20(3).

Regulation, G.D.P., 2018. General data protection regulation (GDPR). Intersoft Consulting, Accessed on October, 24(1).

Saeed, S., Hamawandy, N.M. and Omar, R., 2020. Role of internal and external audit in public sector governance. A case study of Kurdistan regional government. International Journal of Advanced Science and Technology, 29(8), pp.1452-1462.