**Case Study:** Disclosure of sensitive personal data by a hospital to a third party.

Based on the case studies shared during the Collaborative Learning Discussion 3, I noted a common theme: most compliance failures were due to policies and process gaps than technology deficiency.

The General Data Protection Regulation (GDPR) requires entities to protect the personal data and privacy of European Union (EU) citizens. It is a legal framework and applies to any organisation that handles the data of EU citizens (Rossow, 2018). According to GDPR Principles, it requires explicit consent and justification (Intersoft Consulting, N.D.).

Based on the case study, a patient's medical report was disclosed to a third party due to a human error. A staff member deviated from a standard procedure for issuing a report using a non-windowed envelope, and the address was hand-written on the front. However, the staff member who had addressed the envelope manually made an error on the address. Due to the address error, the report was delivered to a third party. The report contains the patient's medical results and the name of a General Practitioner (GP). The sensitive personal data shared with the third party without the patient's consent resulted in GDPR non-compliance.

The correct procedure for issuing medical reports was briefed to the administrative staff to ensure that windowed envelopes would be used to issue reports in the future.

As an information security manager, I would implement a digital delivery method with multifactor authentication to mitigate the issue.  This will ensure secure delivery to the patient and eliminate potential human errors (Berge, 2019).

As the world is working on the pandemic recovery, the governments around the world are actively working on "vaccine passports" that enable the citizens to prove they have been vaccinated. People will be required to disclose personal health information and their vaccine status. The sensitive personal data collected must be protected, and vaccine passports must be implemented in compliance with applicable laws, regulations and industry standards (OPC, 2021).

As shared with the tutor during the collaborative discussion, it is not enough to remind the employees about the principles and articles. Organisations should consider integrating security practices and regulatory requirements such as GDPR within their policies, standards, and procedures. And enforce them by periodic training and security audits to minimise security breaches and non-compliance with regulatory requirements.

**References:**

Berge, J. (2019) Digital Transformation to Reduce Human Errors. Available from: [**https://www.linkedin.com/pulse/digital-transformation-reduce-human-errors-jonas-berge/**](https://www.linkedin.com/pulse/digital-transformation-reduce-human-errors-jonas-berge/) [Accessed 16 July 2021]

Data Protection Commission. (N.D.) Case studies. Available from: [**https://dataprotection.ie/en/pre-gdpr/case-studies#201705**](https://dataprotection.ie/en/pre-gdpr/case-studies#201705) [Accessed 16 July 2021]

Rossow, A. (2018) The Birth Of GDPR: What Is It And What You Need To Know. Available from: [**https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=44aaf23655e5**](https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=44aaf23655e5) [Accessed 16 July 2021]

Intersoft Consulting. (N.D.) Art. 7 GDPR Conditions for consent. Available from: [**https://gdpr-info.eu/art-7-gdpr/**](https://gdpr-info.eu/art-7-gdpr/) [Accessed 16 July 2021]

OPC. (2021) Privacy and COVID-19 Vaccine Passports. Available from: [**https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d\_20210519/**](https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210519/) [Accessed 16 July 2021]