Unit 5 - e-Portfolio Activity - GDPR Case Studies

This case study that I had chosen was from the year 2014, Case study 5: Disclosure of Employee Salary Details by the HSE (2014) that illustrates the importance of the protection of personal data, even if that personal data is being used in a court for evidence. It highlights the rights of the claimant due to the personal data being obtained without permission and prior consent.

What is the specific aspect of GDPR that your case study addresses?
Subsection 2(1)(c)(ii) - Protection of personal data.
Disclosure of employee salary details by the Health Service Executive (HSE) on two separate occasions to a third party (complainant Ex-Wife). The complainant's Ex-Wife had received the personal data of her ex-husband upon request to HSE, this personal data was then used in court as evidence towards ongoing maintenance issues. She was able to provide his P60 and his salary details for the previous 4 months.

How was it resolved?
The complainant refused a letter of apology and opted to seek formal a decision from the data protection commissioner. The commissioners decision was that “The HSE contravened Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003”. (DPC, 2014)

Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003 outlines that data shall not be further processed in a manner incompatible with the purpose for which it was obtained.

Although this case took place in 2014, Amended legislation to this very subsection in 2020 would mean that the same outcome is likely and rules have not changed, even with the UK GDPR framework after exiting the EU. (Legislation, 2022)

Steps I would take as an Information Security Manager to mitigate the issue?
As the information security manager, there are several frameworks or approaches and policies that the company could ensure are in place and which I could follow. One approach to mitigate the risk of breaching Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003 would be to implement and enforce policies and procedures that ensure the security and confidentiality of personal data. This could include measures such as regularly training employees on data protection and security, reviewing and updating security systems and controls, implementing access controls to prevent unauthorized access to personal data, and regularly conducting risk assessments to identify and address potential vulnerabilities (ISO, 2022).

We should also prioritize working closely with our legal and compliance teams to ensure that our organization's data protection policies and procedures are in line with updated, relevant laws and regulations nationally and internationally. This can be managed by the implementation of an certified and audited information security management system (ISO, 2022) and relevant scope.

References

DPC (2014) The Data Protection Commission: Pre-GDPR Case studies. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies#201404 [Accessed on 10 December 2022]

ISO (2022) 27001 Information security management systems. Available from: https://www.iso.org/standards.html [Accessed on 10 December 2022].

Legislation (2022) The data protection, privacy and electronic communications (Amendments etc) (EU Exit) Regulations 2019. Available from: https://www.legislation.gov.uk/uksi/2019/419/regulation/2 [Accessed on 10 December 2022]