Unit 5 E-Portfolio Activity – GDPR

2014 Case study 15: Employee of Financial Institution Resigns Taking Customer Personal Data.

- **Summary of the Case:** The GDPR office got a notification from a Data controller in line with the Personal Data Security Breach Code of Practice stating that an ex-employee had emailed a spreadsheet containing customer's details to personal email address.
- **Findings:**

1. **Workplace policy**: The organisation operates BYOD (Bring Your Own Device) system.
2. **Context of the email (Asset):** Customer's employment details, salaries, contact details and medical consultant.
3. **Compliance with GDPR:** The data controller notified the Office once the data protection policy breach was discovered and details of the ex-employee was provided inclusive of home address.
4. **Follow up action:** The organisation sought assistance from the Office on how to advise their members on mitigations against subsequent incident.

Activity questions and responses:

Q1. What is the specific aspect of GDPR that your case study addresses?

Response: GDPR policy on BYOD and protection of personal data**.**

Q2. How was it resolved?

Response: Plaintiff perspective-

1. The office did an independent search through the Companies Registration Office and found out that the ex-employee operates a Data Controller business from the home address.
2. A further engagement based on the right of operating as a Data Controller and violation of policy of not obtaining consent from former employer to process any personal data got from them revealed that the ex-employee operated under the workforce policy of BYOD which gave him the right with handle business dealings with personal device.
3. However, the ex-employee confirmed that the new business has not started canvassing for clients and that all data in related to former employer has been deleted.

Secondly compliant perspective-The office further engaged the Data Controller on the confirmation of the security policies and procedures in place to protect consumer's data in possession.

The following measures were in place:

1. It was confirmed that the employment contract contained appropriate data-protection clauses.
2. An introduction of software application to password customer's personal data from being emailed.
3. A new policy that all employees must return data and stop further processing upon termination of employment.

Q3. If this was your organisation, what steps would you take as an Information Security Manager to mitigate the issue?

Response: Mitigation on BYOD to ensure compliance of the GDRP policy in relation to personal data protection and Confidentiality are as follows:

- Set a policy that employees use a VPN (virtual private network) when accessing company data which the data is expected to be encrypted to protect against interception by unauthorized user.
- Install mobile device management software on all BYOD devices. This will allow the IT department to remotely wipe the device if it is lost or stolen.
- Train the employees on security procedures like consequence of sharing passwords, downloading email attachments from unknown sources and avoid public Wi-Fi networks.
- Deletion of company data upon termination of the employment relationship.
- Enforce strict password policies, such as requiring employees to use strong passwords, regular change of password and Multiple Authentication factor.
- Regularly scan BYOD devices for malware and other security threats.
- Set up a comprehensive BYOD policy that outlines acceptable use and security procedures.

Conclusion:

The GDPR binds a controller to implement appropriate technical and measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems. The GDPR states that personal data should not be kept for longer than necessary, and time limits should be established for erasure of data. An employer must thus put in place appropriate record keeping practices which are followed by employees. This will ensure that any personal data processed while in business is not retained for longer than necessary on any of the employees' personal devices used for work purposes (Zammit.A).

Reference.

- CEI(9 March 2023),BYOD Security Risks and How To Protect Your Business.Available from: https://copycei.com/byod-security-risks-and-how-to-protect-your-business/[Accessed 8 September 2023].

- University Of Essex Lecture cast(Unit 5) Security and Risk Management Standard .Available from:https://www.my-course.co.uk/mod/scorm/player.php?a=11784&currentorg=articulate_rise&sco

id=23626&sesskey=XGB0F8qmeD&display=popup&mode=normal [Accessed 8 September 2023].

- Zammit .A,2019),Data Protection Implications of a Bring Your Own Device Policy, Available from: https://www.lexology.com/library/detail.aspx?g=93dd3d7e-a863-4bc6-b875-fb453b4b5682 [Accessed 8 September 2023].