GDPR Case Studies

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

  My Case study was based on Prosecution of Guerin Media Limited. This organisation breached several GDPR principles. The first was the Lawfulness, fairness, and transparency principle. The individuals had never conducted any business with the company, so no consent was given to the company to make use of the data. There was no valid reason for company to hold this email address making it unlawful to send emails to the individuals and as the users were not aware there was no transparency that data was being held by the company until the email was received

  The second breach was Purpose limitation. The individuals were not aware why the company would hold work email.

  The third breach s data minimization. If the company was holding email address what confidence does the individual have that they are not holding additional information such a phone number, home address, age and other important details

  The fourth breach is Accountability individuals requested they be removed from emails however this we never performed

- How was it resolved?

  Several fines were issued to the company, each of €1,000, i.e., a total of €4,000.

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

  I would perform a number of checks on any historical data and ensure any new information being obtained has consent from an Individual informing them that we hold data on the user outlining what the data is being held for what reason and for how long we will retain the information. A key aspect is how this data is being used and if this changes they will be notified. I would also ensure an automatic email was sent out to all users reminding them we hold this data every 6 – 9 months and if nothing heard back the assumption that the information held was up to date and accurate and they have provided consent to continue using the data and if not they should notify us to remove this information or opt via email.

  https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/#the_principles