<u>Case Study 1</u>: Marketing offences by MTS Property Management Limited – prosecution

We received a complaint in February 2013 from an individual who received marketing SMS messages from MTS Property Management Limited advertising the company's property-management services. The complainant informed us that she had dealt with the company on one occasion over five years previously, but she did not consent to her mobile phone number being used for marketing purposes. She also pointed out that the SMS messages that she received did not provide her with a means of opting out.

Our investigation of this complaint became protracted as the company denied knowledge of the mobile number to which the SMS messages were sent, and it denied knowledge of the account holder of the sending phone number. However, our investigation established sufficient evidence to satisfy itself that MTS Property Management Limited was responsible for the sending of the marketing SMS messages to the complainant. We decided to prosecute the offences.

MTS Property Management Limited had come to our attention previously in the summer of 2010 when two individuals complained about unsolicited marketing SMS messages sent to them without consent and without the inclusion of an opt-out mechanism. Following the investigation of those complaints, we warned the company that it would likely face prosecution if it committed further offences under Regulation 13 of SI 336 of 2011 at any future time.

At Dublin Metropolitan District Court on 23 February 2015, MTS Property Management Limited pleaded guilty to one charge of sending an unsolicited marketing SMS without consent and it pleaded guilty to one charge of failing to include an opt-out mechanism in the marketing SMS. The Court convicted the company on both charges, and it imposed two fines of €1,000 each. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

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

The case study addresses aspects of the General Data Protection Regulation (GDPR) related to consent and opt-out Mechanism.

GDPR mandates that personal data must be collected and processed with explicit consent from individuals. The complaint in the case study involved marketing SMS messages sent without the individual's consent, which directly contravenes GDPR requirements. It also requires that individuals can withdraw their consent at any time. The SMS messages in the case study lacked an opt-out option, which is necessary for compliance.

- **How was it resolved?**

Despite initial denial, the investigation confirmed that the company was responsible for the unsolicited messages. The company was prosecuted under relevant regulations and fined €2,000 for the infractions. The company also agreed to cover the prosecution costs.

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

Steps as an Information Security Manager:

1. **Implement Consent Management Systems**: Ensure that there are robust systems in place to obtain and manage consent for marketing communications. This includes clear, explicit consent mechanisms and regular audits to confirm compliance.

2. **Develop and Enforce Policies**: Create and enforce internal policies that comply with GDPR requirements, including those related to marketing communications. Regularly review and update these policies to address new regulations or changes.
3. **Training and Awareness**: Conduct regular training for staff on GDPR compliance and data protection best practices. Ensure that all employees are aware of their responsibilities related to handling personal data and obtaining consent.
4. **Opt-Out Mechanism**: Ensure that all marketing communications include a clear and easy-to-use opt-out mechanism. Regularly test and review this process to ensure it works effectively.
5. **Regular Audits**: Perform regular audits of marketing practices and data handling procedures to identify and address any potential issues before they lead to violations.
6. **Documentation and Reporting**: Maintain thorough records of consent and marketing communications practices. Be prepared to provide documentation in case of an audit or investigation.
7. **Data Protection Impact Assessments (DPIAs)**: Conduct DPIAs for any new marketing strategies or systems to assess potential risks and ensure compliance with GDPR before implementation.

By taking these steps, an Information Security Manager can help prevent issues related to GDPR compliance and protect the organization from potential fines and legal actions.