GDPR Case Studies:

My Case Study:

Case Study 3: The Dublin Mint Office Limited

The DPC received a complaint on 13 October 2017 from an individual who had received two marketing telephone calls that same day, one targeted at him and one at his son, from The Dublin Mint Office Limited. The caller in each case had attempted to sell commemorative coins. In his complaint, the complainant explained that he had registered online a few months earlier with the company for an online offer on his own behalf and on behalf of his son, providing the same telephone contact number for both during the online registration process. The complainant stated that he ticked the marketing opt-out box during that online registration process.

During the course of the DPC's investigation, The Dublin Mint Office Limited admitted that it had made the marketing telephone calls. It explained that when the complainant supplied his telephone number during the online application process in May 2017 the order form had only offered an opt-in option to receive marketing mails and emails. The company confirmed that the complainant had not selected the opt-in option and he was therefore marked as opt-out for marketing mails and emails only. The company explained that a gap in the system in place at the time only allowed for an opt-in to marketing mails and emails but that it was not an opt-out for telesales. As a result, the complainant's details were included in a list for a follow-up telesales call. The company informed the DPC that it had written to the complainant to apologise for the inconvenience caused to him and to his son by its inadvertent mistake.

The DPC had previously issued a warning to The Dublin Mint Office Limited in September 2017 concerning other complaints which had been made to the DPC concerning unsolicited marketing communications by the company. The DPC therefore decided to prosecute The Dublin Mint Office Limited. At Dublin Metropolitan District Court on 14 May 2018 the company pleaded guilty to two charges in relation to both marketing telephone calls. It also agreed to cover the DPC's prosecution costs. In lieu of a conviction and fine, the Court applied Section 1(1) of the Probation of Offenders Act. (Commsion, 2018)

The case study illustrates the continued usage of personal data even after an individual has expressly declined to receive promotional mailings. Here, the company manipulated the lack of a clearly defined "opt out" option for tele sales calls to their benefit. This is an example of intentionally misleading a user. After receiving several reports and concerns from users, the DPC conducted a thorough preliminary investigation and determined that the company had illegally handled the personal data of millions of users for telemarketing purposes. The DPA discovered, among other things, that individuals had received promotional calls from The Dublin Mint Office Limited that were not requested and were sometimes recorded. Even after asking The Dublin Mint Office Limited to remove their information, some data subjects continued to receive marketing calls. It also promised to pay for any legal fees incurred by the DPC. The Court substituted probation for conviction and a fine under Section 1(1) of the Probation of Offenders Act.

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

The access right is important to the General Data Protection Regulation (GDPR). First, since only the right of access permits the data subject to exercise other rights (such as rectification and erasure). On the other side, omissions or incomplete disclosures are subject to penalties.

The response to a right of access request consists of two phases. First, the controller must determine whether or not any of the data subject's personal information is being processed. In any instance, a positive or negative outcome must be reported. If the answer is affirmative, the second level includes a vast array of facts. The right of access includes information about the processing purposes, the categories of personal data processed, the recipients or categories of recipients, the planned duration of storage or criteria for their definition, information about the rights of the data subject such as rectification, erasure or restriction of processing, the right to object, instructions on the right to lodge a complaint with the authorities, and information about the origin of the data, as long as it is reasonably possible to ascertain such information. Last but not least, if personal data are transported to a third country without an adequate level of security, data subjects must be informed of all precautions that have been implemented.

Depending on the circumstances, information may be disclosed to the data subject in writing, electronically, or orally in accordance with Article 12(1), sentences 2 and 3 of the GDPR. According to Article 12(3) of the GDPR, information must be delivered without undue delay and within one month at the latest. This one-month deadline may be extended only in justified circumstances. Generally, the information must be offered without charge. If

additional copies are needed, one may seek a fee that is commensurate with administrative expenses. The controller may also deny a data subject's right of access request if it is unfounded or excessive. If the controller is processing a large volume of information about the data subject, he also has the right to request that the data subject clarify their request in terms of specific data processing or kind of information. (Consulting, 2020)

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

The GDPR stipulates that the "Information to be Disclosed to the Data Subject" must be provided no later than the first time an individual is contacted using their data. Consequently, we would offer this information on the individual's first connected call, but there will undoubtedly be exceptions to this norm.

We would employ a three-pronged strategy. Data Protection Statements will be incorporated into regular confirmation or verification statements for successful conversations where a purchase is placed, or an ongoing relationship is otherwise established with the customer. This could occur before or after the start of the ordering process in order to collect extra information.

During the "End Call Politely" phase, more information on "data protection requirements" will be sent to the consumer if they choose not to proceed. It is unlikely that many clients will want to listen to a legal statement if they are eager

to hang up, but the phrasing of paragraph 3 of Article 14 indicates that you must make the offer. We shall always note that the information is available on the company's website to remain compliant without needlessly requiring agents to read a long data protection statement.

Lastly, you must provide your agents with access to the whole statement at any time throughout the call, should the client request additional information on how you obtained their data, what data you have kept on them, or what you intend to do with their data. In the weeks and months following the GDPR's implementation, it's probable that consumers across the EU will become much more data-savvy, and your agents may be constantly questioned about how your organization saves, processes, and protects individual data. Having this information readily accessible to your agents and providing them with the required training can help reduce agent and customer complaints. (Jarvis, 2017)

References:

(Commsion, 2018) URL: https://www.dataprotection.ie/en/pre-gdpr/case-studies#201803

(Consulting, 2020) URL: https://gdpr-info.eu/issues/right-of-access

(Jarvis, 2017) URL: https://callcentresoftware.co.uk/blog/2017/december/rights-and-responsibilities-gdpr-compliance-scripts-for-call-centres/