Although GDPR regulations provide much-needed structure to data processing, they also enforce restrictions which require careful attention for compliance to be maintained due to their rigid nature. One example of this is a case brought to the Data Protection Commissioner (DPC) in 2017, where the principle of purpose limitation was breached during a dispute, despite a seemingly valid case existing for the offending company. The case centered around two parts: the first part was that a company's employee went to work on the site of an external toll company. The employee threatened the toll company, which the toll company recorded on CCTV. The toll company then contacted the person's employer and asked them to not send that specific employee to the site again, which the employer agreed to. The toll company thereafter considered the situation resolved. The second part of the case is that, approximately 2 months later, the person's employer contacted the toll company and asked for the recorded CCTV footage, to which the toll company agreed. This caused the employee to lodge a case with the DPC, as the employee argued that this disclosure was done without his consent. The toll company argued it was in their legitimate interest to process the data because of the nature of the threats and risk of damage to their property.

This scenario was resolved in favour of the employee, but not just because of the lack of consent. After investigation, the commission determined that the processing of the employee's data was initially acceptable for the purposes of enforcement (i.e. making the request to forbid the employee from the site). However, it determined that there was no valid legal basis for releasing the data in the second part of the events. This was because the toll company considered the matter settled 2 months ago, and consent had not been obtained for the new purpose of processing (i.e. providing a copy of the data to the employer). Furthermore, the employee was not well-informed of how their data would be managed on site (e.g., being informed that their CCTV footage could be processed, and the reasons it may be processed). Based on the above, the company lacked an adequate legal basis to process the employee's data in this way.

If I were the Information Security Manager for the offending company, I would take a multifaceted approach to mitigating the issue. Based on the conclusion of the DPC, the toll company made an error in judgement when using "legitimate interest" as a basis for sending the employee's data because the facts of the matter contradicted this basis (Data Protection Commission, 2020). If the issue was considered resolved and 2 months had passed without any amendments or adjustments, it cannot be said that there is still a "legitimate interest" for processing the data again. The first correction to be made is therefore to introduce an internal review process when determining a legal basis for responding to any request- depending on the size of the company, resources available, and the nature of the problem, this could be as simple as using an interactive tool provided by the ICO (n.d.a), or having a more expansive review based on expert opinion. The second and third problems go hand-in-hand: the existing list of purposes for data processing may be too limited in scope (because the process of disclosure in this case required additional consent), and the physical site itself does not have enough detailed information on how visitors' data is collected and processed, which assists in meeting the right to be informed (ICO, n.d.b). To rectify this issue, discussions should be held where stakeholders discuss and anticipate how data might need to be processed in new ways to meet new requests, and once these situations are discovered, they must be clearly communicated to a visitor on site through signage or similar.

**References**

Data Protection Commission. (2020) Case Studies. Available from: https://dataprotection.ie/en/pre-gdpr/case-studies [Accessed 23 January 2021].

ICO. (n.d.a) Lawful basis interactive guidance tool. Available from: https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/ [Accessed 23 January 2021].

ICO. (n.d.b) Right to be informed. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ [Accessed 23 January 2021].