**Unit 3 – Exercise: Security Standards**

1. **Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment? For example, a company providing services to anyone living in Europe or a European-based company or public body would most likely be subject to GDPR. A company handling online payments would most likely need to meet PCI-DSS standards.**

Pampered Pets is a small business based in Hashington-on-the-Water, probably located in the UK, and it specialises in selling high-quality pet foods. The majority of its sales, approximately 90%, occur in-store, while the remaining 10% come through email (My-course, N.D.).

Considering the nature of the business and its operation within the EU, it is highly likely that the General Data Protection Regulation (GDPR) would apply to Pampered Pets. The GDPR sets rules for handling personal data and applies to organisations targeting people in the EU or conducting the personal data of EU residents (Your Europe, 2019). Since Pampered Pets collects and processes personal data through email addresses for orders, it is likely subject to GDPR compliance requirements.

The PCI Security Standards Council is an international organisation that develops and promotes data security standards to ensure safe payments across the globe. These standards protect payment account data and encourage secure payment products and solutions for merchants, service providers, financial institutions, developers, and vendors (PCI Security Standards Council, N.D.). However, since Pampered Pets only receives a small percentage of orders via email for in-store pickup and most of their in-store sales, they do not need to comply with the Payment Card Industry Data Security

Standard (PCI-DSS). The PCI-DSS is a set of security guidelines designed to ensure that companies that handle credit card information maintain a secure environment (Barney, 2023).

Also, Pampered Pets does not handle healthcare data, and the Health Insurance Portability and Accountability Act (HIPAA) does not apply to them, according to Proofpoint (2021). HIPAA mandates security measures for companies that deal with protected health information (PHI), and Business Associates (BAs) are third parties who access patient information to provide services on behalf of HIPAA-bound entities. While HIPAA aimed to reform the health insurance industry, the objectives of increased portability and accountability would have been expensive for the industry. Therefore, Congress introduced measures to combat fraud and abuse and streamline health claims administration, as the HIPAA Guide (N.D.) explained.

2. **Evaluate the company against the appropriate standards and decide how would you check if standards were being met?**

Analysing Pampered Pets' data processing activities about GDPR standards is necessary. This is because they collect customers' email addresses for order purposes and staff personal data for salaries and employment records, and considering it is a shop, they potentially have CCTV footage. Furthermore, according to Veterinary IT Services (N.D.), these data can be categorised as follows:

- Contact information for clients
- Clinical data from patients
- Human resources records
- Employee information
- Supplier details

It is essential to ensure that all these categories of data are processed in compliance with GDPR.

As to the guidelines published by the ICO (2023), a valid legal basis must be established before processing personal data. For instance, the following are the essential GDPR standards, per Irwin's (2021) remark, for determining if Pampered Pets comply with the GDPR:

- It is crucial to ensure that the gathering and use of client data are legally justified and have a clear legal basis, such as obtaining explicit permission from the individuals concerned. Additionally, it is essential to limit the data collection and preservation to only the information necessary to fulfil specific tasks, such as fulfilling customer orders.
- To safeguard the data from unauthorised access or breaches, it is recommended to put adequate organisational and technical measures in place. This can include encryption, password protection, and other security protocols appropriate for processing data.
- Furthermore, individuals have the right to access, correct, delete, and limit the processing of their data. Respecting these rights and taking appropriate measures to ensure these requirements handle the data is essential.
- In the event of a data breach, it is essential to establish processes for detecting and reporting such incidents within the allotted time limits. This can help minimise the breach's potential impact and ensure appropriate actions are taken to mitigate the risks associated with such incidents.

**3. What would your recommendations be to meet those standards?**

To ensure compliance with GDPR requirements, I recommend Pampered Pets conduct a self-assessment to identify gaps between current practices and GDPR requirements. The Approved Contractor Scheme (ACS) ensures public safety and maintains high standards in the private security industry. Security businesses must conform to the ACS standard to demonstrate their capability and effectiveness in protecting people, property, and premises (Security Industry Authority, N.D.). This self-

assessment can help Pampered Pets understand the shop's current level of compliance and identify areas needing improvement.

In addition, as per the Information Commissioner's Office (2018) highlights, I would recommend the following:

- Pampered Pets may also consider an independent audit for a more comprehensive evaluation. An audit can provide a detailed analysis of your shop's compliance with GDPR requirements and identify areas needing further attention.

- To ensure the security and privacy of Pampered Pets clients' data, it is essential to develop and implement a comprehensive data protection policy that outlines the specific data handling practices that Pampered Pets staff will follow. This policy should include steps to obtain explicit client consent for collecting and using their email addresses and establish procedures for handling data subject rights requests.

- To further enhance the protection of Pampered Pets clients' data, Pampered Pets should implement technical safeguards such as password protection and encryption for data storage. These measures will help to prevent unauthorised access to sensitive information.

- It is also crucial to provide data security awareness training to staff, as this will help to ensure that everyone understands the importance of protecting client data and knows how to follow the established data handling practices. This training should cover data classification, secure data storage and transmission, and incident reporting.

- Finally, Pampered Pets should develop a data breach response plan that outlines the steps it will take in the event of a data breach. This plan should include procedures for identifying the scope and nature of the breach, notifying affected individuals and regulatory authorities, and taking steps to mitigate the breach's impact on our clients and business.

**4. What assumptions have you made?**

Firstly, I assumed that the information provided was complete and accurate. Secondly, I thought that Hashington-on-the-Water was located in the UK. Thirdly, I thought they might have CCTV footage since it is a shop. However, upon conducting further

research, I discovered that my assumption regarding the location was incorrect. Despite searching on Google Maps and other online resources, I couldn't find any relevant information about Hashington-on-the-Water.

I would also like to mention that Pampered Pets doesn't seem to have a website or an online store. The only way to place an order with them is through email.

**References:**


- My-course (N.D.). *Risk Identification Report | UoEO*. [online] Available at: https://www.my-course.co.uk/mod/assign/view.php?id=943392 [Accessed 14 Feb. 2024].
- Your Europe (2019). *Data protection*. [online] Your Europe - Business. Available at: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm.
- PCI Security Standards Council. (N.D.). *Standards*. [online] Available at: https://www.pcisecuritystandards.org/standards/.
- Barney, N. (2023). *What is PCI DSS (Payment Card Industry Data Security Standard)? - Definition from WhatIs.com*. [online] Techtarget. Available at: https://www.techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard.
- Proofpoint. (2021). *What Is HIPAA Compliance? HIPAA Laws & Rules | Proofpoint UK*. [online] Available at: https://www.proofpoint.com/uk/threat-reference/hipaa-compliance.
- HIPAA Guide. (n.d.). *HIPAA for Dummies*. [online] Available at: https://www.hipaaguide.net/hipaa-for-dummies.
- Veterinary IT Services (N.D.). *Is Your Veterinary Practice GDPR Compliant?* [online] Available at: https://veterinaryit.services/is-your-veterinary-practice-gdpr-compliant/ [Accessed 14 Feb. 2024].
- ICO (2023). *A guide to lawful basis*. [online] Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/.
- Irwin, L. (2021). *Summary of the GDPR's 10 key requirements*. [online] IT Governance Blog En. Available at: https://www.itgovernance.eu/blog/en/summary-of-the-gdprs-10-key-requirements.
- Security Industry Authority (N.D.). *The SIA Approved Contractor Scheme Interactive Self-Assessment Workbook.* (2022). Available at: https://assets.publishing.service.gov.uk/media/633ec142d3bf7f58719d616e/sia-acs-saw.pdf [Accessed 14 Feb. 2024].
- Information Commissioner's Office (2018). Essential guide to the General Data Protection Regulation (GDPR). *Guide to the General Data Protection Regulation (GDPR)*. [online] doi:https://doi.org/10.1211/pj.2017.20203048.