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.

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

What would your recommendations be to meet those standards?

What assumptions have you made?

1. UK-GDPR (General Data Protection Regulation)

Applicability:

- Since Pampered Pets is based in the UK, the company is subject to the UK General Data Protection Regulation (UK-GDPR), which mirrors the EU GDPR with adjustments post-Brexit. UK-GDPR applies to any organization that processes personal data of individuals located in the UK, including customers' names, contact details, payment information, and any other identifiable information.

GDPR would apply if Pampered Pets:

- Has customers located in Europe (EU/EEA).
- Collects or processes any personal data of individuals within the EU.

Given that the business is selling pet food locally, GDPR may apply if Pampered Pets sells online and targets customers in the EU or collects data from EU residents (e.g., through online sales, newsletters, or customer registrations).

Evaluation:

- **Data Processing Activities:** Assess how Pampered Pets collects, stores, processes, and uses personal data. This includes customer information gathered through online transactions, in-store purchases, or marketing efforts.
- **Lawful Basis:** Ensure there's a lawful basis for processing personal data, such as consent, contract necessity, or legitimate interests.
- **Data Protection Policies:** Review the company's privacy policy to ensure it complies with UK-GDPR requirements, including transparency about data usage and rights.
- **Security Measures:** Check the security protocols in place to protect personal data, such as encryption, access controls, and data minimization practices.
- **Data Subject Rights:** Confirm that Pampered Pets has procedures for handling data subject requests, such as access, rectification, erasure, and data portability.

2. PCI-DSS (Payment Card Industry Data Security Standard)

Applicability:

- PCI-DSS applies if Pampered Pets processes, stores, or transmits credit card information, whether through online sales, in-store transactions, or over the phone.

Evaluation:

- **Payment Security:** Evaluate how Pampered Pets processes payments. Are credit card transactions handled securely, both online and in-store?
- **Compliance Level:** Determine the appropriate PCI-DSS compliance level for Pampered Pets based on the volume of transactions
- **Security Controls:** Review the implementation of security controls, such as firewalls, encryption, and regular monitoring of payment systems.

3. HIPAA (Health Insurance Portability and Accountability Act)

Applicability:

- HIPAA is specific to the United States and applies to entities handling protected health information. Since Pampered Pets is a UK-based business selling pet food, HIPAA is not relevant to its operations.

How to Check if Standards Are Met:

- **UK-GDPR:** Conduct regular audits of data processing activities, ensure privacy notices are compliant, and verify that data subject requests are handled appropriately.
- **PCI-DSS:** Perform security audits on payment systems, review compliance with PCI-DSS guidelines, and ensure any third-party processors are PCI-compliant.

Recommendations:

1. **UK-GDPR Compliance:**
    - Conduct a data protection impact assessment (DPIA) to identify and mitigate any risks related to personal data processing.
    - Ensure that customer data is collected, processed, and stored in accordance with UK-GDPR, with a clear lawful basis and secure handling procedures.
    - Regularly update privacy policies and procedures to reflect any changes in data protection laws or company practices.
2. **PCI-DSS Compliance:**
    - Ensure that all payment processing is done through PCI-compliant systems and that any stored payment data is encrypted and secure.
    - Implement strong access controls and regular monitoring of payment systems to detect and respond to any security threats.

Assumptions:

- Pampered Pets processes customer data, particularly for online or in-store sales.
- The business accepts credit card payments, either online or in-store.
- The business does not handle health-related data that would invoke HIPAA, nor does it operate in a region where HIPAA is applicable.

References:

ICO. (2020) *UK GDPR guidance and resources*. Available from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ [Accessed 03.09.2024]

PCI Security Standards Council. (2024). *PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs*. Available from https://www.pcisecuritystandards.org/ [Accessed 03.09.2024]

HIPAA. (2020). *HIPAA for Dummies – HIPAA guide*. Available from https://www.hipaaguide.net/hipaa-for-dummies/ [Accessed 03.09.2024]