Exercise: Security Standards

Review the following links/ websites and answer the questions below.

ICO. (2020) **Guide to the General Data Protection Regulation (GDPR)**.

PCI Security Standards.org. (2020) **Official PCI Security Standards Council Site - PCI Security Standards Overview**.

HIPAA. (2020) **HIPAA For Dummies** – HIPAA Guide.

- 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?

My Answers:

1. *Which of the standards discussed in the sources above would apply to the organisation discussed in the assessment?*

Standard	Applicability	Explanation
GDPR	Yes	Pampered Pets is likely based in the UK (Hashington-on-the-Water), and handles personal data (emails, transactions), so GDPR applies.
PCI-DSS	No	The business does not process online card payments and seems to take in-person payments only. PCI-DSS is

		likely not required, unless this changes.
HIPAA	No	Pampered Pets does not deal with medical or health information as defined under U.S. law.

Table 1: Applicability of security standards to Pampered Pets.

From the details in Table 1, it is clear that **only GDPR is relevant to Pampered Pets**. PCI-DSS compliance would become needed once they start accepting online payments or storing card holder data electronically.

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

From the information given,the personal data that Pampered Pets likely handle includes (1) Customer names and email addresses (for email orders), (2) Digital sales transaction records (linked to customer purchases) and (3) Possibly employee records (HR/payroll/tax purposes). The table below shows how Pampered Pets handling of personal data evaluates against GDPR principles.

Principle	Evaluation
Lawfulness, Fairness & Transparency	Unclear if customers are informed how their data is used. No mention of a privacy notice.
Purpose Limitation	Data is likely used only for order processing — compliant.
Data Minimization	Only essential data (email, items ordered) is collected — compliant.
Accuracy	Relies on customer-provided info — mostly compliant.

Storage Limitation	Unknown if data is regularly cleaned or deleted.
Integrity & Confidentiality	Wireless network and old hardware could be vulnerable. No mention of encryption or backups.

Table 2: Pampered Pets data handling evaluated against GDPR

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

   Here are my recommendations for Pampered Pets to meet GDPR requirements:

   - Create a simple privacy notice and make it available to customers (e.g., in-store poster or printed leaflets).
   - Ensure all computers and smartphones are password-protected and updated with security patches.
   - Install antivirus and firewall protection on all computers.
   - Regularly back up key data (sales records, warehouse spreadsheet).
   - Train staff briefly on basic data protection: don't share customer info, keep devices secure, and delete old records.
   - Encrypt sensitive data if stored on disk or backed up to USB/cloud.
   - Define a simple data retention policy, e.g., delete inactive email orders after 6 months.

4. *What assumptions have you made?*
   - Pampered Pets does not sell online (yet), so no e-commerce or cardholder data is stored or transmitted.
   - They are based in the UK, so GDPR (and UK GDPR post-Brexit) applies.
   - Staff may not have formal IT or data security training.
   - Email orders involve minimal personal data (likely just email + pet product).