# Applicable Standards

**UK GDPR:**

UK GDPR Applicability The UK GDPR applies to Pampered Pets because it processes personal data as a controller. According to Article 4 of the UK GDPR, the company qualifies as a data controller as it determines the purposes and means of processing personal data. This includes customer contact information for orders and the new automated warehouse systems. The expansion to serve European customers, including Prince Albert 2nd of Monaco, means the company must also consider EU GDPR compliance, as Article 3 specifies that the regulation applies to companies offering goods to data subjects in the EU.

**PCI-DSS:**

PCI Security Standards Applicability The PCI Security Standards are relevant because Pampered Pets processes payment card data throughout the payment lifecycle. The standards documentation specifically states that these apply to "organizations involved in payments, such as merchants," which describes Pampered Pets' role in processing customer payments both in-store and potentially online with their expansion.

# Compliance Evaluation Framework

For UK GDPR compliance evaluation, the following key areas require assessment:

Data Protection Principles (Article 5) The company must demonstrate compliance with fundamental principles including:

* Lawfulness, fairness and transparency in data processing
* Purpose limitation for customer data collection
* Data minimization in automated warehouse systems
* Accuracy of stored customer information
* Storage limitation with defined retention periods
* Integrity and confidentiality, particularly for high-profile clients

Security Measures (Article 32) Current security measures fall short of requirements, particularly:

* The unsecured wireless network used by staff
* Basic computer systems for warehouse management
* Lack of documented security procedures

For PCI compliance, evaluation should focus on:

* Payment data protection throughout the transaction lifecycle
* Security of payment processing systems
* Implementation of secure practices within the organization

# Recommendations

Based on the regulatory requirements, Pampered Pets should:

1. **Data Protection Infrastructure**

* Implement encryption for personal data storage and transmission
* Establish secure networks with appropriate access controls
* Deploy security monitoring systems
* Create data backup and recovery procedures

1. **Documentation and Policies**

* Develop records of processing activities (Article 30)
* Create privacy notices for customers
* Establish data protection impact assessments for new processing
* Document international data transfer mechanisms

1. **Security Protocols**

* Implement PCI-compliant payment processing systems
* Establish secure communication channels between international locations
* Create incident response procedures
* Deploy access control systems for automated warehouses

# Key Assumptions

The analysis assumes:

1. The current basic IT infrastructure will require significant upgrading to meet both UK GDPR and PCI requirements
2. The automated warehouses will process substantial amounts of personal data
3. High-profile customers will require enhanced security measures beyond standard requirements
4. International operations will necessitate formal data transfer mechanisms
5. The company will need to appoint data protection personnel

This analysis is grounded in specific requirements from the UK GDPR and PCI Security Standards documentation, particularly focusing on the security principles outlined in Article 32 of the UK GDPR and the PCI Standards' emphasis on protecting payment data throughout its lifecycle. The recommendations aim to bring Pampered Pets into compliance while supporting its expansion plans and maintaining its reputation for quality and security.