**Foreword**

This note gives preliminary advice regarding Ludens' claims against Shikari following a data breach involving Ludens' proprietary and sensitive data stored on Shikari's servers. It outlines potential defensive arguments Shikari may use to rebut Ludens' claims, assesses the legal obligations of both parties, and identifies next steps to prepare for litigation.

**Key Facts**

1. **Data Breach Occurrence**: A security breach occurred on Shikari’s servers, resulting in unauthorized access to data stored on behalf of Ludens.
2. **Theft from Servers**: Allegedly, the breach led to the theft of data, including trade secrets, potentially sensitive personal health information, and other proprietary information of Ludens.
3. **Data Stored**: Shikari stored health-related data (possibly anonymized or pseudonymized), trade secrets related to Ludens' diagnostic tools, and other commercially valuable information.
4. **Ludens’ Claims**: Ludens asserts that the data breach caused significant damages, including loss of trade secrets, breach of data protection laws (e.g., GDPR), reputational harm, and economic losses.

**Executive Summary**

**Summary of Findings**  
Shikari can rely on several defensive arguments to resist Ludens’ claims:

1. **Trade Secret Protection**: Ludens must demonstrate sufficient measures to protect the confidentiality of its trade secrets. Shikari can argue the absence of reasonable protective measures or a lack of causation between the breach and the alleged harm.
2. **Data Privacy and GDPR Compliance**: Shikari may argue it was acting as a data processor under Ludens’ instructions and that any breach resulted from inadequate directions or security measures mandated by Ludens.
3. **Limitation of Liability Clauses**: If the contract between Ludens and Shikari limits liability for breaches, this could restrict Ludens’ claims.
4. **Data Classification**: If the data was anonymized and aggregated, Shikari may not be liable under GDPR as anonymized data does not qualify as personal data.

**Next Steps**

* Request all agreements governing the relationship between Shikari and Ludens.
* Seek technical details of the breach and evidence of measures taken by Shikari to secure the data.
* Ascertain the exact nature of the stolen data and Ludens’ claims of damage.

**Defensive Strategy**

**1. Trade Secret Claims**

**Grounds of Claim**: Ludens claims theft of proprietary diagnostic tools and commercial know-how, asserting they qualify as trade secrets.

**Defensive Arguments**:

* **Inadequate Protective Measures**: Ludens must demonstrate it implemented adequate steps to maintain the confidentiality of its trade secrets. Shikari can argue that Ludens’ security measures (e.g., failure to encrypt sensitive data) were insufficient.
* **Public Domain Information**: Diagnostic tools protected by published patents are not trade secrets as they are already publicly available.
* **Lack of Causation**: Shikari can argue that the data breach was caused by factors beyond its reasonable control or due to inherent vulnerabilities in Ludens’ systems.

**Next Steps**:

* Request a list of the allegedly stolen trade secrets and evidence of protective measures.
* Analyze patent records to identify which aspects of the diagnostic tools are publicly available.

**2. Breach of Data Protection Laws (e.g., GDPR)**

**Grounds of Claim**: Ludens alleges a breach of GDPR resulting in unauthorized access to personal health data.

**Defensive Arguments**:

* **Data Classification**: If the data was fully anonymized, Shikari can argue it does not qualify as personal data under GDPR.
* **Processor Liability**: Shikari acted as a data processor under Ludens' instructions. Any deficiencies in security protocols should be attributed to Ludens as the data controller.
* **Compliance with Instructions**: Shikari can demonstrate compliance with Ludens’ data storage and processing instructions to deflect liability.

**Next Steps**:

* Obtain the Data Processing Agreement (DPA) to clarify roles and responsibilities under GDPR.
* Confirm whether the stolen data was anonymized, pseudonymized, or identifiable.

**3. Breach of Contract**

**Grounds of Claim**: Ludens asserts Shikari breached its contractual obligations by failing to prevent the data breach.

**Defensive Arguments**:

* **Limitation of Liability**: Review the contract to determine whether liability for data breaches is capped or excluded under specific circumstances.
* **Force Majeure Clause**: If the breach resulted from extraordinary circumstances, Shikari may invoke a force majeure defense.
* **Adherence to Obligations**: Shikari can demonstrate it adhered to industry standards for data security, shifting responsibility to external factors.

**Next Steps**:

* Analyze contractual terms to identify limitation or exclusion clauses.
* Gather records of Shikari’s security protocols to benchmark against industry standards.

**4. Reputational Harm and Economic Loss**

**Grounds of Claim**: Ludens claims reputational and financial damage from the breach.

**Defensive Arguments**:

* **Speculative Damages**: Shikari can argue that reputational harm or loss of business is speculative without tangible evidence.
* **Contributory Negligence**: If Ludens failed to implement adequate security measures, Shikari can assert contributory negligence.
* **Mitigation of Damages**: Ludens must demonstrate steps taken to mitigate losses post-breach.

**Next Steps**:

* Request evidence of alleged damages, including financial records and market impact analysis.
* Investigate any contributory actions or omissions by Ludens.