Dear Shikari Inc.,

I am from clifford chance and would like to assist you regarding the defensive stratergy you need to follow in order for you to stand against your client Luden's claims referring to the data breach that occurred on your server recently.

Problem sum-up:

- The data breach occurred was un intentional and heavy data loss has occurred including Luden Inc.'s data
- The data theft might have included commercial technical and health care data
- The data that shikari stored was Luden's proprietary technology and hardware that is uses that provides services to its users
- Now that the data breach has occurred and Luden's data might have exposed, He claims against shikari so that his loss is re-paid

Executive Summary (Docs and agreements required):

A data breach has occurred at Shikari's data warehouse and one of its clients, Luden's data was exposed. This is voilation under breach of confidence and data protection claims. I would like to ask Shikari to provide all types of leagal documents and agreements attested and approved so far between Shikari Inc. and Luden Inc. in order to examine the extent of relation between them. I would also request shikari to issue a soft copy of all the security policies and technologies implimented pertaining to be useful in case of advanced study for rebuttal of a potential argument agianst a claim.

There seems to be two main GDPR regualation voilations:

a. Breach of Confidence Claim
b. Data Protection Claim

Defensive Strategy:

Breach of Confidence Claim

- This claim lies on Commercial and technical grounds of the client.
  Commercial grounds include the personal data of the client Luden's users who are the data subject in this case. This includes sensitive information reagrding the data subject viz outlining markerting stategies, sales and turnover per financial year with respect to financial data and exposure. Whereas the *Technical grounds* pertain to the eqipment and the diagnostic tools used by the client to treat their patients for which they hold patent rights

- Potential arguments rebutting the claim are essential when the claim turns into a litigation. They may include:

    - Find if any for the citations in the Trade Secret or some sort of End User agreement between Shikari and Luden regarding the data protection agreements and the technologies used in order to defend against any potential cyber attack. It clearly is the evidence that the technology used could not stand against the immense attack and the client willingly agreed to make a contract knowing its risks.
    - Even though the data breach has occurred, the technical team might be on its way to defend the database and take remedial actions pertaining to get the data back so that minimal damage has incurred due to the attack. All necesssary actions have been taken to immediately address the data leak and sieze the leak so that the leak is isolated and closed. Encrypted form of data that is stored in the data base preserves intergrity of the data so that the secreacy of data is maintained and even in the event of data loss it wouldn't pose a problem if proper encryption methods

- The court might order Shikari to extract and return the data that's breached or at the very least destroy the data if possible in order to avoid data misuse.

Breach of Data Protection Claim

- This claim lies on the grounds of data breach of the consumers of the data subject. The breach was regarding the health data pertaining to patients who had been diagonised and treated with Luden's tools. This is a liability under the GDPR article -5 for having failed to putin place the necessary security measures aimed at preventing unauthorised data procesing
- Potential arguments rebutting the claim are essential when the claim turns into a litigation. They may include:
    - Most of the data now-a-days is encrypted while stored. So if the data that Shikari stores in his data warehouse contains is encrypted or anonomised, as per Article -4 definition of GDPR clearly its not personal data. Hence, there is no question of personal data being breached.
    - Now there may be a statement of anonomised data being a trade secret. But since its confidential and isnot intended to be publicly available, its encryption should be strong enough to hold its confidentiality
    - Now that we are dealing with personal data of clients wrt health care, the data controller and data processsor held incharge of data monitoring are questionable. Since Ludens access the data and process the data, progress and results of patients and their data in order to gain insights of

sales and marketing, as per Article -4 of GDPR Luden is clearly the data controller. If shikari is, the data procesor then if there is any agreement that depicts there is a formal disclosure of data when requested by the controller it would end the issue saying that a Processor is to abide by the instructions of its controller.

- In case the above arguments can't be proven affective against the litigation appealed by the client, then the court may order Shikari Inc., to cover the financial losses incurred due to the data breach vis-a-vis Breach Of Data Protection and Breach Of Confidence claims.

Thanks and Regards
Ramakanth