

Dear Shikari Inc.,

I am Srimoyee from Clifford Chance and would like to assist you regarding the defensive strategy 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 unintentional 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 it uses that provides services to its users

Now that the data breach has occurred and Luden's data might have been 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 a violation under breach of confidence and data protection claims. I would like to ask Shikari to provide all types of legal 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 implemented pertaining to be useful in case of advanced study for rebuttal of a potential argument against a claim. There seems to be two main GDPR regulation violations: 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 regarding the data subject viz outlining marketing strategies, sales and turnover per financial year with respect to financial data and exposure. Whereas the Technical grounds pertain to the equipment 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 necessary actions have been taken to immediately address the data leak and seize the leak so that the leak is isolated and closed. Encrypted form of data that is stored in the data base preserves integrity of the data so that the secrecy 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 diagnosed and treated with Luden's tools. This is a liability under the GDPR article -5 for having failed to put in place the necessary security measures aimed at preventing unauthorised data processing

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 anonymised, 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 anonymised data being a trade secret. But since its confidential and is not 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 with respect to health care, the data controller and data processor held in charge 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 processor 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.

Thank you.

Warm Regards,

Srimoyee Dutta.