Dear client,

Greetings of the day.

My name is Srimoyee and I am here to help you through your request of your video game's database data exposure threat. As per GDPR (General Data Protection Regulation), this obligates to a notification obligation

That you should be aware of few keywords. Controllers shoulder the highest level of compliance responsibility. They must comply with, and demonstrate compliance with, all the data protection principles as well as the other UK GDPR requirements. They are also held responsible for the compliance of their processor(s). They also have to pay Data Protection fee unless exempt. Processors do not have the same obligations as controllers under the UK GDPR and do not have to pay a data protection fee. However, if you are a Processor, you do have a number of direct obligations of your own under the UK GDPR though they are not that diverse as a consumer. Producers are exempted from any data protection fee.

The controller team has to notify superior authority regarding the occurred data breach without any delay within 72 hours of timeframe from the point where they have identified a potential threat of data exposure. If the data leak is massive and is likely to pose a threat to customer's personal data, then the users should be notified regarding the incident. Cautionary measures like changing credentials of any accounts associated with the game in the past can be suggested to win trust of the users to an extent. An investigation team has to be deployed in order to deep dive into the breach and find the severity of occurred breach. This helps us in making the decision of reporting either the superior authority or the customers or both.

Make sure the deployed team is proficient in doing its assigned task. Make sure employers are up to date with aspect to updating data protection regulations and compliances. Make sure to put trust in operations team in order to obtain maximum throughout and to report any issues without border misses. Restrict access and auditing is necessary. Notify the ICO regarding

Last but not the least, the ramifications that result in the event of violation of a notification obligation are severe. Failing to notify the Information Commissioner's Officer (ICO) within the prescribed timeframe may result in heavy fine up to £8.7 million or 2 per cent of your global turnover. Additional litigations other than fine may be imposed with additional prowess of the ICO. It is important to make sure you have a robust breach-reporting process in place to ensure you detect, and notify breaches, on time and to provide the necessary details, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If you decide you do not need to report the breach, you need to be able to justify this decision, so you should document it.

I would like to conclude that make sure you stay complied with the regulations and laws of GDPR in order to keep your organization, its reputation and your client's on safe side. Feel free to reach out for further assistance if required.

Thank you.

Warm Regards,

Srimoyee Dutta.