Great New Games' data protection officer

Dear Mr. Arthur Dent,

Your Firm, Great New Games,The web shop contains a database holding customer information, including names, address information and credit card information for more than 2.5 million customers. And During a scheduled software update you discovered that the data of your 4,000 customers was publicly available for a period of up to six days. The database was unencrypted and available to possibly anyone to access until the latest database update, at which point the data leak was closed. And you have no information whether there was an unauthorised database access whilst the database was unencrypted.

As your customers consented in the processing and saving of the aforementioned data under the EU General Data Protection Regulation (GDPR). This incident may affect the confidentiality and availibility of personal data resulting to a personal data breach.

Recital 87 of the UK GDPR says that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Recital 85 of the UK GDPR explains that:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

So, on becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen. A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO. The main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

If you decide not to notify individuals, you will still need to notify the ICO unless you can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. You should also remember that the ICO has the power to compel you to inform affected individuals if we consider there is a high risk. In any event, you should document your decision-making process in line with the requirements of the accountability principle.

The information you provide to individuals when telling them about the breach.You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of any data protection officer you have, or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.
- If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:
- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

Last but not the least, the ramifications that result in the event of voilation of a notification obligation are severe. Failing to notify the Information Commisioners Officer (ICO) within the prescribed timeframe may result in heavy fine upto £8.7 million or 2 per cent of your global turnover. Additionals 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 regualtions 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 futher assistance if required.
Thanks and Regards

Gevendra Kumar Sahu