**Subject:** Assessment of GDPR Notification Obligations

Dear Client's Name,

Thank you for reaching out regarding the recent incident and its potential legal implications under the General Data Protection Regulation (GDPR). Based on your inquiry, I have assessed the situation to determine whether notification obligations apply and, if so, to whom notifications must be made. Below, I outline the legal framework, conditions for notification, and potential risks of non-compliance.

**1. Summary of Findings**

Based on the information provided, the situation may involve a personal data breach as defined under the GDPR. If this is confirmed, there are notification obligations under Articles 33 and 34 of the GDPR. Specifically:

* **To the supervisory authority:** Notification is required under specific conditions within 72 hours of becoming aware of the breach.
* **To affected individuals:** Notification is required when the breach is likely to result in a high risk to their rights and freedoms.

**2. The Legal Framework**

**2a. Key Definitions**

* **Controller:** An entity that determines the purposes and means of processing personal data.
* **Processing:** Any operation performed on personal data, such as collection, storage, or dissemination.
* **Personal Data Breach:** A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

**2b. Does This Constitute a Personal Data Breach?**

Under GDPR, a breach occurs if there is any compromise to personal data's confidentiality, integrity, or availability. Examples include unauthorized access, loss of devices containing data, or exposure to malware.

If your incident involved personal data being exposed to unauthorized parties or compromised in a way that risks individuals' privacy, it qualifies as a breach.

**2c. Notification to Supervisory Authority (Article 33)**

When a breach occurs, the GDPR mandates notification to the relevant supervisory authority unless it is unlikely to result in a risk to the rights and freedoms of individuals.

**Key requirements:**

* **Timeframe:** Notification must occur within 72 hours of becoming aware of the breach. If delayed, justification must be provided.
* **Content:** The notification must include:
  1. Nature of the breach, including affected data categories and approximate number of data subjects involved.
  2. Contact details for your Data Protection Officer (DPO) or relevant contact.
  3. Likely consequences of the breach.
  4. Measures taken or proposed to address the breach and mitigate potential harm.

**2d. Exemptions**

If it is determined that the breach is unlikely to result in a risk to individuals' rights and freedoms, notification to the supervisory authority is not required. Documentation of the breach and the reasoning for not notifying is essential for accountability purposes.

**3. Notification to Data Subjects (Article 34)**

Notification to individuals is required if the breach is likely to result in a high risk to their rights and freedoms (e.g., risk of identity theft, financial loss, or reputational damage).

**Key requirements:**

* **Content:** The notification must include the nature of the breach, contact information for assistance, likely consequences, and measures taken to mitigate risks.
* **Exemptions:** Notification to individuals is not required if:
  + Data was encrypted or otherwise rendered unintelligible to unauthorized parties.
  + Measures have been taken to mitigate the high risk to individuals.
  + Notification would require disproportionate effort (in which case, a public notice may be issued instead).

**4. Legal Enforcement and Risks of Non-Compliance**

Failure to comply with notification obligations can result in:

* **Fines:** Up to €10 million or 2% of the total worldwide annual turnover for less severe breaches. Serious breaches may attract fines of up to €20 million or 4% of global turnover.
* **Reputational Damage:** Non-compliance can erode trust with clients and partners.
* **Litigation Risk:** Affected individuals may seek compensation for damages.

**Recommendations**

To ensure compliance and minimize risks:

1. **Verify the Breach:** Confirm whether the incident qualifies as a personal data breach under GDPR.
2. **Document Details:** Record the breach, investigation findings, and risk assessment.
3. **Notify the Supervisory Authority:** If applicable, ensure notification within the 72-hour timeframe.
4. **Communicate with Affected Individuals:** If high-risk conditions apply, prepare clear, timely, and transparent communications.
5. **Review Security Measures:** Identify and implement measures to prevent recurrence.

Please let us know if you require assistance in preparing notifications, conducting risk assessments, or communicating with stakeholders.

Best regards,  
[Your Full Name]  
[Your Position]  
[Your Contact Information]