Date: [Insert Date]
To: [Data Subject Name]
Address: [Data Subject Address]

Data Breach Notification Letter

Re: Notification of Personal Data Breach in accordance with Article 34 of the GDPR

Dear [Data Subject Name],

We are writing to inform you of a recent data breach that may have involved your personal data. Protecting your information is very important to us, and we are committed to keeping you informed and providing guidance on how you can protect yourself.

What Happened?

On [date of breach], we became aware of a security incident, where [brief summary of the nature of the data breach, e.g., "unauthorised access to our systems was detected"]. The breach was identified and contained on [date].

What Information Was Involved?

The incident involved the following types of personal data: [List specific data types, e.g., names, email addresses, physical addresses, account information, etc.]. No financial information, such as bank account or credit card details, was affected. / [Or specify if financial/other sensitive data was affected.]

What We Are Doing

Upon discovery, we took immediate steps to investigate and contain the breach. We have implemented additional security measures and are working closely with data protection authorities. We have also reported the incident to the relevant supervisory authority in accordance with GDPR requirements.

What You Can Do

As a precaution, we recommend you:

- Monitor your accounts for any unusual activity
- Be alert to suspicious emails or correspondence
- Consider changing affected passwords
- Contact us or relevant authorities if you notice anything concerning

Contact Details

If you have any questions or need further information, please contact our Data Protection Officer:
Email: [DPO Email]
Phone: [DPO Phone]
Address: [Company Address]

Sincerely,

[Your Name]

[Position/Title]

Important Notes

- This notification is required by GDPR when a personal data breach poses a high risk to individuals' rights and freedoms.
- The letter should be clear, concise, and include all relevant facts known at the time.
- Maintain documentation of the breach and communication process as proof of compliance.
- Prompt action and transparency can mitigate reputational and legal risks.
- Continued monitoring and communication may be necessary as more information becomes available.