Over Parish Council Personal Data Breach Policy

Introduction

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Identifying a personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
Recital 87 of the GDPR makes clear 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.

Considerations to be made when reporting a Personal Data Breach

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms

- If it's likely that there will be a risk then you must notify the ICO
- If it's unlikely then you don't have to report it
- Document your decision even if you do not report it to the ICO

Assessment of Risk

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

- Will the risk have adverse effects on individuals, which include emotional distress, and physical and material damage.
- Will the risk only cause possible inconvenience to those who need the data to do their job.
- You need to assess this case by case, looking at all relevant factors.

e.g Can the breached data be used to commit identity fraud, if yes then this would need to be notified, given the impact this is likely to have on those individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list.

On becoming aware of a breach

You should try to 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.

Data Processor responsibilities

If external processor's suffer a breach, then under Article 33(2) they must inform you without undue delay as soon as they become aware.

Reporting time restraints

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

When reporting a breach

you must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach
- including, where appropriate, the measures taken to mitigate any possible adverse effects.

Action to be taken if full details not known

it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

Action to be taken by Controllers

Controllers must

- prioritise the investigation
- give it adequate resources
- expedite it urgently
- notify the ICO of the breach when you become aware of it
- submit further information as soon as possible.

How to notify a breach to the ICO?

- use the online reporting form S55
- or call the helpline 0303 123 1113
- or email casework@ico.org.uk

Notifying individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals you must inform those concerned directly and without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

- assess both the severity of the potential or actual impact on individuals as a result of a breach
- assess the likelihood of this occurring
- If the impact of the breach is more severe, the risk is higher
- If the likelihood of the consequences is greater, then again the risk is higher

In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

Information to provide to individuals when informing them of a 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 your data protection officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach
- the measures taken to mitigate any possible adverse effects.

Other steps needed in response to a breach

You should ensure that you record all breaches, regardless of whether or not they need to be reported to the ICO.

You may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

Failure to notify

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined with the ICO's other corrective powers under Article 58.