MENHENIOT PARISH COUNCIL
www.menheniotparish.org.uk

Briefing Note

GDPR Reporting data breaches policy

1.0 Background

1.1 The GDPR is based on six principles that govern the way in which personal data is collected, stored, managed and disposed of. Personal data 'should be processed in a manner that ensures appropriate security and protection'. However, the ICO[1] recognises that security and protections may not always be 100% perfect, and so public bodies are required to have policies in place to support reporting and remedial action.

1.2 A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. The council needs to have the right procedures in place to detect, investigate and report a breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. The council needs to be able to demonstrate that it has appropriate security, technical and organisational measures in place to protect against a breach.

2.0 Outline Proposals

2.1 If there is no risk of harm to an individual (for example because some low risk data has been inadvertently released or made public such as an email address) then this type of breach would not need to be reported. Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported.

2.2 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.

2.3 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. The council must ensure it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not it needs to notify the relevant supervisory authority and the affected individuals.

2.4 Council must also keep a record of any personal data breaches, regardless of whether they are required to notify.

3.0 Precautions to take

3.1 Councillors, staff, contractors and the council's data processors should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs. This is covered in the council's Acceptable Use Policy and will be included in all future contracts that the council agrees.

3.2 Examples of personal data breaches and steps to avoid them include:

- Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
- The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary.

[1] Information Commissioners Office

- Lost memory sticks which contain unencrypted personal data – The council should put protocols in place for memory stick usage
- Malware (IT) attach – ensure up to date anti-virus software is in place.
- Equipment theft – check security provisions.
- Loss of personal data which is unencrypted
- The rights of individuals to have their personal data protected extends to their right to privacy, and not being named during public meetings where councillors have been advised not to.

3.0 Sources

3.1 The policy has been extracted from the NALC GDPR Toolkit (updated August 2018), guidance from the ICO and Simon Mansell, Corporate and Information Governance Manager & Data Protection Officer, Cornwall Council.

Author : John Hesketh, Parish Clerk, Responsible Financial Officer & Data Protection Officer
Date: 25 September 2018