Lower Hardres & Nackington Parish Council
GDPR Implementation & Compliance
Data Breach Policy Document

Compiled – Mike Taylor – August 2018

Introduction

Under the General Data Protection Regulation (GDPR") introduced on 25 May 2018, data controllers such as councils and parish meetings have new obligations to:-

(i) Keep an internal record of all personal data breaches
(ii) Report them within 72 hours to the ICO in certain circumstances
(iii) Notify an individual affected by a personal data breach in certain circumstances. Data processors will also have a new obligation to notify the data controller of a personal data breach without delay.

A personal data breach may have significant consequences for an individual whose data is affected. Personal data breaches may also cause reputational damage for the councillor parish meeting responsible for the breach. In addition, failure to report a breach may result in intervention by the ICO which includes a fine up to €10 million.

This document summarises the data breach reporting obligations and how we will respond to a personal data breach should it occur.

a) What is a personal data breach?

GDPR defines this as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4). Examples of a personal data breach 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; and
- loss of availability of personal data.

Lawful handling of personal data includes taking steps to reduce the risk of the occurrence of personal data breaches. GDPR specifically requires data controllers and data processors to implement appropriate technical and organisational measures to ensure appropriate levels of security against the risks presented by processing personal data. The risks include the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data (Articles 5 and 32) . The measures set out in GDPR include:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

b) Consequences of a personal data breach

Personal data is information held by a data controller or processor about an individual which identifies them and may, for example, include contact details, date of birth, bank details, information about their education, health, personal, business or working life or family. A breach of personal data may result in a loss of control over personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of person.al data, damage to property, social disadvantage.

This means that a breach, depending on the circumstances in each case, can have a range of adverse effects on an individual, which include emotional distress, and physical and material damage.

c) Data controller's duty to report a personal data breach to the ICO

Lower Hardres & Nackington Parish Council (The Data Controller) shall notify the ICO about a personal data breach if it is likely to result in "a risk to the rights and freedoms" of an individual. The breach shall be reported "without undue delay and, where feasible, not later than 72 hours after having become aware of it". Where notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay. Data breaches shall be notified to the ICO's website as follows:-

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

If a breach is likely to result in a risk to the rights and freedoms of an individual, notification shall:-

(i) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned

(ii) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained

(iii) Describe the likely consequences of the personal data breach

(iv) Describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

GDPR provides that in so far as it is not possible to provide the information above at the same time, the above information may be provided in phases without "undue further delay".

d) Data controller's duty to notify an individual that a personal data breach has occurred

If the personal data breach is likely to result in "a high risk to the rights and freedoms" of an individual, this shall be communicated to the individual "without undue delay". This communication shall be in clear and plain language and include the nature of the personal data breach and the information set.

Examples of personal data breaches about which an affected individual would need to be notified are below.

- A ransomware attack which results in the council's electronic personal data being encrypted. Back-ups are not available and the data cannot be restored / made available to the council
- An HR file is left on a bus
- The clerk emails a database of council contractors' payee details to the RFO and copies all councillors
- An ex-clerk/councillor refuses to return paper/ electronic files containing personal data
- Unencrypted personal data is emailed to a councillor's personal device and his emails are hacked
- A councillor shares sensitive personal data about a council employee on his Facebook account
- An old council computer which still contains personal data on the hard drive is donated to a local charity

Exemptions from mandate to notify an individual.

There are certain circumstances where there is no mandate to notify individuals. These include:-

- It has implemented appropriate technical and organisational protection measures, and that those measures have rendered the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- it has taken subsequent measures which ensure that the high risk to the rights and freedoms of individual(s) is no longer likely to materialise or
- It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the individual(s) are informed in an equally effective manner.

Even when a data controller is excused from communicating with an individual for the reasons above, the GDPR provides that the ICO, who should already have been notified of the personal data breach, still has the power to require the data controller to inform the affected individual if it considers there is a high risk to the individual's rights and freedoms.

e) Data processor's duty to notify data controller of a personal data breach

GDPR provides that when a data processor becomes aware of a personal data breach, it must notify the data controller of this "without undue delay".

A council may outsource its payroll and or HR functions to a business. In this example, the business would be processing the personal data relating to the council's staff on behalf of the council and is a data processor. If the business suffers a temporary loss of personal data due to a power outage which means it cannot pay salaries on time, the business would need to report this to the council.

f) Data Breach Awareness and Designated Responsibilities

The Lower Hardres & Nackington Parish Councils Data Protection Officer (DPO) shall ensure that the awareness and training provided to all members at the inception of GDPR is continued as required in the future. At any time, anyone should be able recognise a data breach and raise / escalate the consideration of an incident to appropriate person(s) to :-

i) determine whether a personal breach has occurred
ii) ii) respond appropriately.

The Lower Hardres & Nackington Parish Councils Clerk shall be responsible for reporting a data breach. The Clerk may consult with the Chairman, and or relevant committee chairs and, as appropriate, with businesses which provide the council's IT support services and or host and maintain its server. A committee or sub-committee could not be responsible for investigating or responding to personal data breaches because the notice period for convening a meeting is inconsistent with the urgency of the work involved. The persons responsible for responding to breaches may wish to consult with the council's DPO.

g) Data controller's duty to record all personal data breaches

Compliance against the statutory timescale GDPR requires a data controller to keep an internal record of all personal data breaches. This is regardless of whether or not they need to be reported to the ICO. Records shall comprise the facts relating to the personal data breach, its effects and the remedial action taken.

The Parish Clerk shall establish and maintain appropriate records to satisfy the above requirements.