nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

FEBRUARY 2018

L02-18 | REPORTING PERSONAL DATA BREACHES

Introduction

When the General Data Protection Regulation ("GDPR") is introduced on 25 May 2018, data controllers such as councils and parish meetings will 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 and (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 council or 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 briefing i) explains the new personal data breach reporting obligations , ii) encourages councils and parish meetings to ensure that there are organisational and technical resources in place to minimise the occurrence of personal data breaches and iii) explains how to respond to personal data breaches when they 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.

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

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 personal 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

GDPR provides that a data controller has an obligation to 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 must be reported "without undue delay and, where feasible, not later than 72 hours after having become aware of it" (Article 33). Where notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay. To notify the ICO of a personal data breach, please see the ICO's website https://ico.org.uk/for-organisations/report-a-breach/

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

When notifying the ICO of a breach which is likely to result in a risk to the rights and freedoms of an individual, a data controller must:

(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 and
(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

GDPR provides that if a personal data breach is likely to result in "a high risk to the rights and freedoms" of an individual, the data controller must communicate this to him "without undue delay" (Article 34). When communicating with the individual concerned, the data controller must describe in clear and plain language the nature of the personal data breach and provide the information set out in (ii)-(iv) in section c) above .

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;

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

- 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.

GDPR provides that a data controller does not need to communicate with an individual if any of the following applies.

- 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 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) Responding to personal data breaches

Staff, councillors (and parish meeting chairs) ought to able to recognise what may constitute a personal data breach. Awareness and training for this purpose is recommended. Anyone should be able to raise / escalate the consideration of an incident to appropriate person(s) to i) determine whether a personal breach has occurred and ii) respond appropriately.

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

As some breaches may need to be reported by a data controller within 72 hours, it is recommended that each council (and parish meeting) designates person(s), who are available at short notice, with the responsibilities summarised below.

- to promptly investigate potential personal data breaches;
- to respond to personal data breaches discovered by the data controller (including those reported to it by its data processor(s));
- to take steps to address a personal data breach and to mitigate negative consequences and
- to, as appropriate, report a breach to the ICO and the individual(s) affected by the breach.

The designated persons within a council could be the clerk/ RFO who 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.

The ICO's website has prepared two checklists which councils and parish meetings can use to ascertain if they are ready to respond to a personal data breach. These can be accessed via https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

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

GDPR requires a data controller to keep an internal record of all personal data breaches (regardless of whether or not they need to be reported to the ICO), comprising the facts relating to the personal data breach, its effects and the remedial action taken (Article 33). An example of a breach which would not need to be reported to the ICO but would need to be recorded internally is the loss of encrypted personal data on a memory stick.