GDPR Breach Notification Policy

Adopted by Marden Parish Council on: 12th June 2018
Reviewed on: 9th July 2019 / 4th May 2021 / 8th March 2022 / 14th March 2023 / 12th March 2024
Review date: March 2025

Office Opening Times:
Mondays, Tuesdays & Fridays 10am - 12 noon
www.mardenkent-pc.gov.uk
Email: clerk@mardenkent-pc.gov.uk

GENERAL DATA PROTECTION REGULATIONS

BREACH NOTIFICATION POLICY

1 Scope

This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

2 Responsibility

All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and Councillors of Marden Parish Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

3 Procedure – Breach Notification Data Processor to Data Controller

Marden Parish Council shall report any personal data breach to the data controller (Clerk) without undue delay.

Details of all breaches are recorded in the Internal Breach Register.

Notification is made by email, phone call or letter.

Confirmation of receipt of this information is made by email.

4 Procedure – Breach Notification Data Controller to Supervisory Authority

The Clerk shall notify the supervisory authority [ICO] without undue delay, of a personal data breach.

The Clerk assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

If a risk to the aforementioned is likely, The Clerk shall report any personal data breach to the ICO without undue delay, and where feasible not later than 72 hours. Where data breach notification to the ICO is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The data controller (Clerk) shall provide the following information to the Parish Council on a Breach Notification Form:
A description of the nature of the breach
The categories of personal data affected
Approximate number of data subjects affected
Approximate number of personal data records affected
Name and contact details of the Parish Council
Likely consequences of the breach
Any measures that have been or will be taken to address the breach, including mitigation
The information relating to the data breach, which may be provided in phases.
The Clerk notifies the contact within the ICO, which is recorded in the Internal Breach Register

Notification is made by [email, phone call, etc.].
Confirmation of receipt of this information is made by email.

5 Procedure – Breach Notification Data Controller to Data Subject

Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject Marden Parish Council shall notify the affected data subjects without undue delay.

The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above.

Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

The ICO may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.