Susan Ellis: Information Management Consulting

18th July 2022

Stratfield Mortimer Parish Council – Audit of GDPR Compliance

An audit of GDPR compliance can determine whether there are any weaknesses in the way the Parish Council processes personal data. Using the EU checklist for compliance https://gdpr.eu/checklist as a template, I carried out an audit on 18th July 2022 with the Parish Clerk Lynn Hannawin.

Findings

The Parish Council is appropriately registered to process personal data with the Information Commissioner's Office (ICO). I suggested that when the registration is renewed in 2023, my name is added as Data Protection Officer.

The Parish Council has robust processes in place for data security (encryption and password protection) as well as a two stage access to the Office 365 system, which means personal data is held securely on a restricted internal system.

There is a clear and accessible Privacy Policy covering the processing of personal data, but as an advisory I have suggested a line or two is added regarding the Parish Council's cemetery records, as these will be retained for the duration of a fifty year lease, with regular updates to leaseholder information.

The Parish Council has a record retention schedule covering the personal and other data collected – this fulfills the legal requirements under S46 of the Freedom of Information Act 2000 (Code of Practice on Records Management). As an advisory I have supplied a copy of my Parish Council Record Retention template for a comparison of retention periods. The Clerk has a good grasp of retention and deletion processes and older minutes have been sent to the BRO for archiving, in accordance with best practice.

The Parish Council also has a Parishes Record of Processing Activities, as required under GDPR. This includes all the relevant personal data holdings and processing the Parish Council carries out.

The Parish Council regularly backs-up data and holds back-up copies securely. We discussed internal security, and I suggested that the good practice the Parish Council already carries out could be encapsulated in a Security Policy, for future reference by new Councillors and new employees. This would ensure that the good practice currently in place is continued.

We discussed issues around Councillors access to data. There are particular issues with the use of an individual's own devices (laptops, tablets, mobile phones) as these are not usually encrypted. I have agreed to provide guidance produced by the ICO on the security issues of such devices.

We also discussed the problems which can arise when Councillors leave the Parish Council, but still retain emails and documents relating to confidential work within the Parish Council. It was suggested that Councillors regularly delete older emails (enquiries from residents etc.) once the piece of work is completed (a central record should be held by the clerk), and also confidential minutes and papers after two years. This would leave little documentary information to delete once they had completed their term of office. I agreed to provide information leaflets for councillors on GDPR and FoI.

	PHONE	MOBILE	EMAIL
Open View, New Road Hill, Midgham, Berks RG7 5RY	01189712428	07766611705	susancarveth@gmx.com

We discussed the need for a Data Protection Policy. Whilst not a legal requirement this can be a useful addenda for Councillors, staff and the public alike. The Clerk was aware of a useful template shared by another Parish Council and we agreed that I would amend this (it relates to DPA 1998, not GDPR) and it could then be adopted by Stratfield Mortimer Parish Council. I will carry out this piece of work by end July.

We discussed data breaches, and what was likely to be a reportable breach. From the context of the Parish Council's work it is unlikely that the Parish Council will experience a reportable breach. It was confirmed that there has not been a breach in the past.

We discussed the Data Protection Impact Assessment process, and when it might apply. The clerk considered that a planned survey might attract an assessment, and we discussed what personal data might be collected. I agreed to point the clerk to information from the ICO on the Impact Assessment process.

Summary

Stratfield Mortimer's GDPR compliance is excellent. There is good robust security of data with appropriate back-up procedures and secure systems. The clerk has a good grasp of the issues around data protection and how these apply to the data collected. Documentation supporting data protection, including the Privacy Policy, Retention Schedule, and Record of Processing Activities is comprehensive, and the suggestions made for additional documentation will improve this. I anticipate no issues arising with data handling and there is little likelihood of data breaches. Suggestions for advising Councillors of any possible issues with emails and security of confidential data should also ensure the most achievable level of protection, given the Parish Council's limited resources.

Susan Ellis

Susan Ellis: Information Management Consulting