

Ulcombe Parish Council

Data Processor Questionnaire

This document is provided by a Data Controller (Ulcombe Parish Council) to a Data Processor (.....) to comply with the duty of the former to assist with definitions and duties as defined in Recital 95 of the General Data Protection Regulation, with comprehensive coverage within Chapter IV.

Its purpose is to assess the level of compliance within your organisation and to address any areas that require attention prior to May 2018. It may assist you to review as a starting record the compliance that data processors will be required to cover under article 28.

It is our belief that you are a Processor who handles personal data of individuals on our behalf, and as such we are required to enter into an agreement with you. Prior to that we have a duty to ensure the processor's security arrangements are at least equivalent to the security that we are required to have in place as if we were processing the data ourselves. Please refer to the full requirements that we will be asking of you within Article 28 of GDPR.

Please provide the following information on your organisation for record purposes;

Organisation name:

Address:

Post code:

Contact person:

Email address:

Telephone number:

Please advise whether you have a Data Protection Officer, if so supply the following details:

DPO Name:

Email address:

Telephone Number:

To assist us with our own compliance responses, please provide the following information.

- 1 Define where the Data is stored (Please set out details of the database and filing systems containing personal data for the storage of information on behalf of the Data Controller)
- 2 Advise who has permission to access the data, both internally and externally
- 3 How is access to this data logged and controlled?

- 4 How and where is our dataset backed up
- 5 Is the dataset encrypted on your servers?
- 6 If so, when is it decrypted?
- 7 Please advise whether you apply anonymisation or pseudonymisation
- 8 Do you have a retention policy? How long do you keep personal data?
- 9 Are you able to restrict the purposes for which you process the information?
- 10 How often is the personal information you process updated?
- 11 Is any of the information you process known to be incomplete, outdated or wrong?
- 12 Is there any mechanism for data subject to access the data, and if so can they correct it?
- 13 Do you sell, rent, or by any means disseminate the personal information to third parties?
- 14 Do you have any mechanism to check the accuracy and completeness of data?
- 15 Do you have a process to update, correct or delete data?
- 16 Do you operate any regular or automated process to 'clean' your data?
- 17 Does any dataset include personal information on subjects under the age of 16?
- 18 Could the personal data ever get transferred to another party?
- 19 Does the dataset include recordings of video or sound that includes the public?
- 20 Do you maintain a record of processing activities that is frequently reviewed and updated which can be demonstrated to the Data Controller?
- 21 Please confirm that information (digital and manual, and especially special category data) is only stored in your organisation. If a third party (a Sub-Processor) is involved please provide full information.
- 22 Where is archived information stored, in what format and medium? Please provide details of any Sub – Processor as in Question 21.
- 23 Describe the physical, administrative and technological security procedures in operation to keep all information secure.
- 24 Does anybody within or outside your organisation have access to the personal information of the Data Controller? If so, who authorises such access?
- 25 What policies and procedures do you have for detecting and dealing with breaches and can they be identified and reported to the Data Controller within 72 hours?

- 26 What data audit facilities or controls are in place to ensure that there is no internal unauthorised access to personal data?
- 27 How is personal information, including backups and archives, destroyed if you are instructed to do so by the Data Controller?
- 28 Who authorises the destruction and who carries it out?
- 29 What happens to the data at the end of the contract period?
- 30 Are you required to transfer data between departments or to third parties? If so how is the data transferred and what encryption or similar security is deployed?
- 31 Please confirm that no data including archives and backups is transferred outside the UK and EEA.
- 32 Do you have a privacy policy?
- 33 Please confirm that you are prepared to enter into a contract with us as required by GDPR as reproduced below:-

Thank you in advance for your time and support.