General Data Protection Regulation: Data Audit

**Please fill in this form for every type of data you hold – including electronic and paper files.**

|  |  |
| --- | --- |
| Data Auditor: About You | |
| 1. Person completing the form |  |
| 1. Date form completed |  |
| 1. Team/framework |  |
| 1. Do you process personal[[1]](#footnote-1) data on individuals? |  |

|  |  |
| --- | --- |
| Data Collection | |
| 1. Type of data[[2]](#footnote-2) |  |
| 1. Purpose of the data |  |
| 1. Where did you get the data?[[3]](#footnote-3) |  |
| 1. Is any ‘special category’[[4]](#footnote-4) data held or processed? Why? |  |
| 1. Notice given to individual (privacy note, data collection statement). Attach an example copy. |  |
| 1. How often is each notice reviewed or changed (if applicable) and who reviews or changes each notice? |  |
| 1. For each purpose outlined in question 2 (purpose of data), determine which of the lawful processing conditions you think is relied upon for the collection and processing of the relevant personal data.[[5]](#footnote-5) |  |
| 1. Where consent is relied on upon, are your consent forms clear? Will the individual understand what has been consented to? Provide a copy of any consent forms you use. |  |

|  |  |
| --- | --- |
| Storage and Archiving | |
| 1. Where is the data is stored?[[6]](#footnote-6) Is this onsite or with a third party? |  |
| 1. How do you protect that data?[[7]](#footnote-7) |  |
| 1. Is ‘special category data’ held separately from other personal data?[[8]](#footnote-8) |  |
| 1. Do you archive the above data? If yes, what file format is it saved as? |  |
| 1. Where is this archive stored? |  |

|  |  |
| --- | --- |
| Security | |
| 1. Who has access to the personal data you store? Inside and outside the diocese. |  |
| 1. Who authorises such access? |  |

|  |  |
| --- | --- |
| Destruction | |
| 1. How long do you keep the data for? |  |
| 1. How is data destroyed when it is no longer needed? Give details. |  |
| 1. Who authorises the destruction? Who carries out the destruction? |  |

|  |  |
| --- | --- |
| Transfer of Personal Data | |
| 1. Do you transfer this data to other departments/frameworks/third parties outside the diocese?[[9]](#footnote-9) |  |
| 1. How is it transferred? |  |
| 1. Is this on a regular basis? List examples. |  |
| 1. Do you have a formal data sharing agreement or similar (attach a copy for each instance)? |  |

|  |  |
| --- | --- |
| Training | |
| 1. Have you had any data protection training or training in any other relevant law? Describe what it was and when. |  |
| 1. Are you aware that unlawful access to and/or disclosure of personal data is prohibited? |  |

|  |
| --- |
| Comments |
|  |

**Note:** This is intended to provide an overview of GDPR and is not a definitive statement of the law. For a definitive guide, check out the [Information Commissioner’s Office website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr).



1. Anything that identifies an individual. [↑](#footnote-ref-1)
2. Name, address, age, email etc. [↑](#footnote-ref-2)
3. Third party, face to face, phone, email, web etc. [↑](#footnote-ref-3)
4. Medical/health data, ethnic origin, religion etc. [↑](#footnote-ref-4)
5. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

   **(a) Consent:**the individual has given clear consent for you to process their personal data for a specific purpose.

   **(b) Contract:**the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

   **(c) Legal obligation:**the processing is necessary for you to comply with the law (not including contractual obligations).

   **(d) Vital interests:**the processing is necessary to protect someone’s life.

   **(e) Public task:**the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

   **(f) Legitimate interests:**the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides

   those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.) [↑](#footnote-ref-5)
6. Server, personal device, work device, Cloud, outside service, paper, DropBox, Google Group, spreadsheet, text document, database, online, Survey Monkey, other. [↑](#footnote-ref-6)
7. Locked filing cabinet, password etc. [↑](#footnote-ref-7)
8. Medical/health data, ethnic origin, religion etc. [↑](#footnote-ref-8)
9. Third parties include, but are not limited to, The Bishop’s Office, Diocesan & Archdeacons offices, Aquila, Canterbury Diocesan Enterprises, National Church Institutions. [↑](#footnote-ref-9)