# **Organisation Name**

# **How Should We Store Our Data?**

This workbook accompanies our ‘How Should We Store Our Data’ guide. Is it intended to help small charities carry out a simple risk assessment of their data, and plan any actions needed.

There are three parts to the Workbook. Part 1 is a simple template to help you think about how you should secure your data. The loss of different types of data will have different impacts, and so you may need more controls on some than others.

Part 2 is a very simple space for you to note down the high level responses to the question “what do we need to do with this data?”. This is only intended as a starting point for your thinking, not a full requirements specification. Depending on the complexity of your requirements it may be enough before you look at different storage options; or it will be the starting point for a larger piece of work.

Part is just a copy of the ICO checklist for contracts with External Processors. You’ll need to complete these checks if you use any third party data processors.

January 2023

**Disclaimer:** This workbook and the accompanying guides do not constitute legal advice and are not a substitute for your duty to meet your own data protection obligations. These resources are designed as a starting point to assist small and new UK charities in thinking about their legal obligations and practical data needs and are used at your own risk. You should seek advice from a lawyer or data protection professional for further assistance.

## Part 1: A Simple Risk Assessment Template

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Data About Who? | What would be the impact to us if this were compromised in some way? | What would be the impact to the Data Subject if it were compromised in some way? | Do we need any more technical controls (e.g. backups) to protect this data further? | Do we need to change any processes, or carry out training, to protect this data further? | Who’s going to do this? When? |
| Trustees |  |  |  |  |  |
| Staff |  |  |  |  |  |
| Volunteers |  |  |  |  |  |
| Donors |  |  |  |  |  |
| Supporters |  |  |  |  |  |
| Service Users |  |  |  |  |  |
|  |  |  |  |  |  |

## Part 2: What do we need to do with our data?

|  |  |
| --- | --- |
| Data About Who? | What do we need to do with this data? Communicate? Reporting? Case Notes? Sharing? |
| Trustees |  |
| Staff |  |
| Volunteers |  |
| Donors |  |
| Supporters |  |
| Service Users |  |

## Part 3 – GDPR Contract Checklist

Complete this for each contract you have with an External Processor of personal data.

|  |  |  |
| --- | --- | --- |
| Supplier: |  | |
| Contract is for: |  | |
| Date of contract: |  | |
|  | |  |
| The contract (or other legal act) sets out details of the processing including: | | Section of the contract: |
| the subject matter of the processing; | |  |
| the duration of the processing; | |  |
| the nature and purpose of the processing; | |  |
| the type of personal data involved; | |  |
| the categories of data subject; | |  |
| the controller’s obligations and rights. | |  |
|  | |  |
| The contract or other legal act includes terms or clauses stating that: | | Section of the contract: |
| the processor must only act on the controller’s documented instructions, unless required by law to act without such instructions; | |  |
| the processor must ensure that people processing the data are subject to a duty of confidence; | |  |
| the processor must take appropriate measures to ensure the security of processing; | |  |
| the processor must only engage a sub-processor with the controller’s prior authorisation and under a written contract; | |  |
| the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights; | |  |
| taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments; | |  |
| the processor must delete or return all personal data to the controller (at the controller’s choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and | |  |
| the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations. | |  |