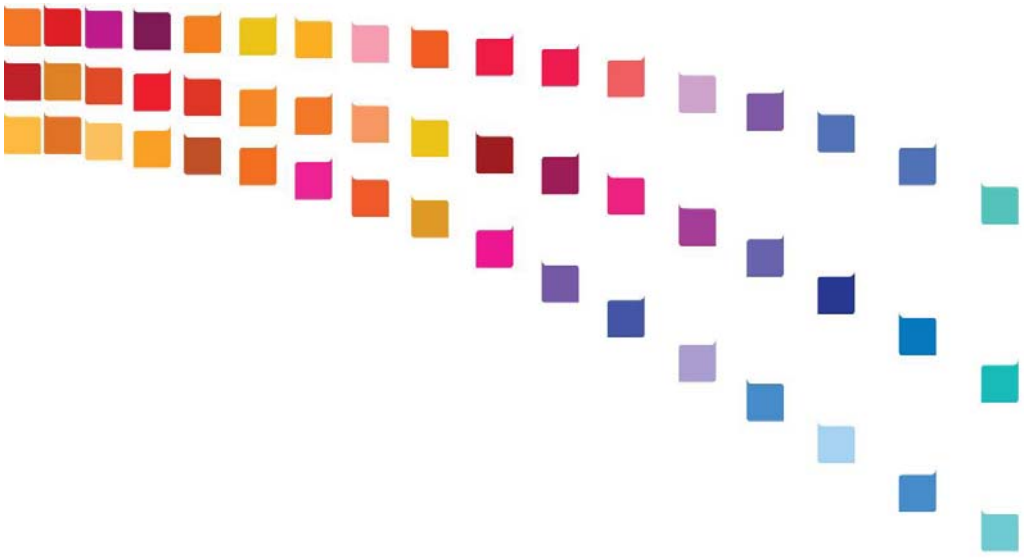
Guidance Notes for DMA Suggested Data Processing Agreement



Guidance Notes for DMA Suggested Data Processing Agreement

General

1. This supplementary contract covers processing of data only. It does not cover issues such as the ownership of data which should already be covered in current contracts.

2. It is not possible to prepare a standard contract relevant to all the wide variety of circumstances likely to be found e.g. in mailing house, computer bureau, list broking, list management outsourcing. These guidelines therefore relate to a supplementary contract adding to the contractual relations already in place (for processing (including the contract price) the additional requirements set out in the Data Protection Act 1998.

3. The purpose of a supplementary contract for processing is to ensure that the data which are subject to processing are no less safe with the data processor than they would be if the processing was undertaken by the data controller himself.

4. The supplementary contract for processing can be used either by a data controller outsourcing to a data processor or a data processor secondary outsourcing work to a sub processor, provided the required changes are made as highlighted in the comments on the template. In the case of secondary outsourcing there must be a supplementary contract for processing between the data controller and the data processor. The data processor will become the data controller for the purposes of the sub- processing but only with regard to the transfer of data to the sub- processor. The data processor must check that their contract with the data controller allows them to outsource to a sub-processor and that, if required by the contract with the data controller, the appropriate consents have been obtained.

5. The Data Protection Act 1998 Schedule 1 Part II paras 9 – 12 sets out the interpretation of the 7th Principle which reads:
    i. "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

6. Para 11 of Schedule 1 Part II requires the data controller to choose a data processor providing sufficient guarantees in respect of technical and organisational security measures governing the processing, and to take reasonable steps to secure compliance with those measures.

7. Para 12 says that the contract must be made or evidenced in writing and must provide that the data processor is to act only on instructions from the data controller.

8. Para 10 requires the data controller to take reasonable steps to ensure the reliability of its employees who have access to the data and para 12 (b) requires the contract to ensure that the data processor gives equivalent undertakings.

9. The security measures, taking account of "the state of technological development and cost of implementation," must ensure a level appropriate to the harm that might result and the nature of the data to be protected.

10. When choosing a data processor the data controller should take out references and make other enquiries, e.g,. whether they are members of a recognised trade body, to establish the processor's bona fides.

Terms in Supplementary Contract

a) name and address of both parties

b) clear delineation of the precise nature of the processing to be carried out, emphasising that the data processor must not take any action outside the description of processing laid down.

c) details on three separate issues

I. reliability of staff used by the data processor. This will in practice require staff entering into confidentiality undertakings as part of the terms and conditions of working

II. technical measures taken by the data processor to avoid the possibility of unauthorised or unlawful processing or accidental loss, destruction or damage of the data concerned. This might involve written protocols to address access eg. password control, encryption, tracing, verification of parties communicating data, and the like. The data controller should consider asking the data processor to confirm that it has appropriate insurance cover against loss or damage to the data by any means should be considered.

III. Organisational measures taken by the data processor – these include

- is access to the building or room controlled or can anybody walk in?
- are the precautions against burglary, fire or natural disaster adequate?
- can casual passers-by read data off screens or print-outs?
- are back-up copies of the data stored separately from the live files?
- is there a procedure for cleaning tapes and disks before they are re-used or is new data merely written over the old? In the latter case is there a possibility of the old personal data reaching somebody who is not authorised to use it?
- is printed material containing information extracted from personal data disposed of securely? Often it will be appropriate to dispose of printouts by shredding.
- is there a procedure of authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?
- is responsibility for the data processor's security policy clearly placed on a particular person or department?
- are breaches of security properly investigated and remedied – particularly when damage or distress has been caused to an individual?

d) the liability of the data processor for any misfeasance, loss or damage should be limited to an amount agreed to by the parties, and could be insured.

Overseas Processing

In assessing the appropriateness of using a data processor in a third country (i.e. outside the European Economic Area (EEA), the 27 Member States of the European Union, plus Iceland, Liechtenstein and Norway) consideration should additionally be given to the political and legislative environment in which the data processor operates.

Sensitive Data

If sensitive data are to be processed the level of security should be greater than for non-sensitive data.