



OP SIS Practice Management Solutions Ltd.

Support and Data Conversion Policy and Agreement with regard to the Data Protection Act 1998

As a software house we naturally have to perform work of a support or conversion nature on the databases that our software products use.

In some instances this will require our customers to send a backup copy of a database to OP SIS' offices for us to fix a problem, or so we can upgrade or convert the database from one software format to another. We may also need to remotely access your computer system for the purpose of supporting our software products.

During the course of these services we do not normally "control" or "process" (change) any personal information held in the database.

Since the majority of our customers are within the legal profession and record personal information about their clients in our software databases, they will usually be registered as **Data Controllers** under the *Data Protection Act 1998*, and according to the *Seventh Principle* of the Data Protection Act 1998 Legal Guidance document it is the responsibility of that Data Controller (you, as our customer) to ensure adequate security measures are taken by OP SIS in the handling of that data.

We recommend this is accomplished by drawing up an appropriate contract specifying the required security measures and precautions you (in your capacity as Data Controller) require of OP SIS to safeguard the information.

To assist with this we have provided this basic contract for you to give permission to OP SIS so that we may perform the required services on the data you control.

➔ *Please note that this is only a basic template and you should provide your own contract if you feel it does not accurately state the terms and conditions you require.*

OP SIS Practice Management Solutions Ltd take similar precautions as outlined in the *Seventh Principle* to ensure the security of any data whilst in our possession.

Please note that OP SIS Practice Management Solutions does not perform "data processing" as defined by the Data Protection Act 1998. We merely take actions on the database "wrapper", not on the actual content of the database, i.e. OP SIS does not control, amend, delete or otherwise change any information records that may be construed as "personal information". The only circumstance we might become "data processors" would be if expressly instructed to amend "personal information" by you, the Data Controller.

For more information concerning the Data Protection Act see the government web site at  www.dataprotection.gov.uk.

Please do not hesitate to contact our Helpdesk if you need any further information or assistance regarding technical/hardware matters:-



England, Scotland & Wales: +44(0)1780 766300

Northern Ireland: +44(0)28 9065 3006

Republic of Ireland: +353(0)1 294 2903

<http://www.opsisltd.com/>



Agreement re Data Protection Act 1998

OPSIS Practice Management Solutions Ltd., agree to provide the service stated below according the terms of this agreement, which are based upon the Seventh principle of the Data Protection Act 1998 which states;

"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."

OPSIS Practice Management Solutions will:-

1. Take reasonable steps to ensure the reliability of employees having access to any database to which the Data Controller has permitted access, and that those employees are aware of their responsibilities and that all regular data care procedures are fully and conscientiously followed.
2. Where possible and appropriate ensure that product databases will be password-protected to prevent unauthorised access, whilst in the possession of OPSIS at their offices, and during electronic transfer from customer to OPSIS, or between OPSIS premises, to be effected either by means of master database passwords or by compression into a password-protected archive for the duration of the transfer.
3. Will allow only the relevant OPSIS personnel access to User level passwords disclosed by the the data controller for the purpose of accessing and working with the data using the appropriate software, and such password information will be kept securely at the OPSIS premises according to the company information security policy.
4. Ensure adequate security measures are taken at the OPSIS premises to prevent unauthorised access to offices or rooms containing sensitive personal information, and to ensure that casual passers-by are unable to read personal information showing on screens or documents.
5. Upon completion of the service and when instructed to do so by the Data Controller, OPSIS will destroy copies of the data, including any printed material showing personal information by shredding, and return any associated media. OPSIS reserve the right to retain certain data, or printed material of a technical nature that would aid future product support.
6. Not change, delete, or add any personal information records contained within the data, nor distribute any of the same personal information to any other party, except upon the express written instruction of the Data Controller.
7. Whilst OPSIS maintains a daily rotational backup schedule, in some instances of the provision of fast-turnaround support services the data supplied by the Data Controller may not be included in the normal backup schedule. Otherwise OPSIS will endeavour to include the supplied database in our normal backup routines.
8. Provide adequate protection against corruption by viruses and other forms of intrusion, by means of appropriate network security, firewall and data scanning software.
9. Where data is required to be passed to a third party for processing, OPSIS will ensure that the Data Controller is informed so that a written contract can be put in place which states that the agent will work within the Data Controllers data protection policy. "Control" of the data will not be allowed to move to the third party.
10. In the event that a laptop computer is necessary for the transfer, use or demonstration of the service provided and contains data provided by the Data Controller, the laptop computer shall be password protected and "locked" if the OPSIS employee leaves the laptop unattended at any time.
11. Under no circumstance will OPSIS allow any data to be transferred to countries outside the EU.
12. OPSIS shall not be liable to the Data Controller for any loss or damage whatsoever or howsoever caused, arising directly or indirectly in connection with this Agreement, other than to the liabilities of OPSIS as set out in the terms and conditions of the separate Software License Agreement or Service Level Agreement, and other than as imposed by Law.

**The Data Controller (Customer) agrees that:-**

13. They are a Data Controller fully registered with the Information Commissioners offices for the Data Protection Act 1998.
14. The Data Controller acknowledges that it is the ultimate responsibility of the Data Controller to define a procedure covering the temporary removal of personal data from the data controllers premises, according to and including any other obligations of the Data Protection Act 1998, and the Data Controller agrees that any procedural items not mentioned in this agreement are the sole responsibility of the Data Controller to define and specify.
15. In the case of an electronic transfer being used to send data to OPSIS and to receive data back, it is the responsibility of the Data Controller to ensure adequate security measures are taken. Where electronic transfer is deemed possible but may be considered insecure that instead the data will be saved to a suitable backup media and transferred by an appropriately insured postal service at the cost of the Data Controller.
16. Data backup procedures normally performed by the Data Controller on their premises will continue to be done even during any down-time while waiting for the service to be completed, and no reliance is made on OPSIS for restoring data that should have been backed up by the Data Controller.
17. After sufficient time has elapsed for the Data Controller to check the service has been completed satisfactorily, it is the sole responsibility of the Data Controller to instruct OPSIS to destroy any remaining copies of the data in its possession and to return any media associated with the service performed, except where retaining certain items of a technical nature will aid future support services provided by OPSIS.



OPSIS Practice Management Solutions Ltd.
Support and Data Conversion Policy and Agreement
with regard to the
Data Protection Act 1998

Please note that this is a basic contract and you should provide your own contract if you feel it does not accurately state the terms and conditions you require.

Please complete this form and fax back to OPSIS (Fax No. 01476 567716). We will counter-sign and fax a copy back to you.

Company Name (Data Controller):

Address:

Telephone Number:

FAX Number:

Service being provided (please tick/describe):

Support: Conversion: Other:

Opsis Log / Job No:

Software Product:

Solicitor Case Manager: Millennium/Solo: Other:

Database Name/Location:

The Data Controller hereby grants OPSIS Practice Management Solutions Ltd permission to perform the service stated on the data provided, according to the terms described on all pages of this agreement, in conjunction with any Software License Agreement or Service Level Agreement currently in effect between the two parties.

Date of Contract:

Name:

Signed (Data Controller):

Signed (for OPSIS):