Data Sharing Agreement Between

The Property Ombudsman

And

Member and Registered Agents

1. Partners
The Partners to this Agreement are The Property Ombudsman (TPO) and the Member and Registered Agents (property agents registered with TPO). By registering with TPO, Member and Registered Agents agree to be bound by the terms of this Agreement.

2. Purpose
TPO scheme is designed to reach a resolution of unresolved disputes in full and final settlement. It provides consumers (who may be actual and potential buyers, sellers, landlords, leaseholders, lessees and tenants of property or have been otherwise involved by the actions of an agent) with free and independent redress of complaints relating to acts or omissions of Member and Registered Agents in connection with the sale and/or purchase and/or letting and/or management of property in the United Kingdom, Channel Islands and the Isle of man. The scheme will also provide that redress to small commercial enterprises and charities. In order to do this, TPO needs to collect information from Member and Registered Agents by obtaining their company files. The information may from time to time include personal data for the purposes of the data legislation.
This Agreement sets out the framework for the sharing of personal data between the parties as Data Controllers. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

3. Potential Recipients
Member and Registered Agents will share information with TPO, who may subsequently share it with complainants in order to explain the Ombudsman’s judgement, if it is appropriate and lawful to do so. TPO may also share the information with the TPO Council and other competent authorities such as Trading Standards or any recognised regulatory or trade organisation or otherwise as set out in TPO’s Privacy Policy.

4. The Data to be Shared
Member and Registered Agents will share their company files (which may include personal data) with TPO for the purpose of conducting a review of the complaints submitted by the complainants and/or for another compatible purpose. Member and Registered Agents are required to comply with the DPA applicable national data protection laws and guidance in sharing information and they must ensure that it is fair and lawful to do this in each case. TPO expects that, in most cases, the data subjects concerned will have a reasonable expectation that their information will be provided to TPO for the purpose of processing a complaint or another compatible purpose. However, in some cases, it may be necessary for a Member or Registered Agent to obtain specific consent from relevant data subjects and in other cases the Member and Registered Agent may need to rely on an exemption under the DPA applicable national data protection laws and guidance. Member and Registered Agents will be required to explain the legal basis for any information missing or redacted from a company file.

5. Data Quality
Member and Registered Agents will ensure that all information shared is accurate and up to date.

6. Data Security
Regardless of the type of information being accessed, processed and stored, security is considered of paramount importance. All personal data held by TPO is held securely. Electronic personal data is held on secure servers and encrypted memory sticks and manual data is held in locked cabinets in locked and alarmed premises.

As data controllers for the data they collect, all Member and Registered Agents are expected to treat personal data in accordance with the DPA applicable national data protection laws and guidance and ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Member and Registered Agents are themselves responsible for complying with security in respect of the DPA applicable national data protection laws and guidance, irrespective of the specific terms of this agreement.
7. **Data Retention and Deletion**

The recipient of the information shall either return or destroy the information once processing of the information is no longer necessary for the purposes it was originally shared for.

8. **Data security breaches and reporting procedures**

Having considered the applicable national data protection laws and guidance, the parties have in place their own guidance that must be followed in the event of a data security breach. For the purposes of this Agreement, a data security breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the information.

Parties are under a strict obligation to notify any potential or actual losses of the information to the other as soon as possible and, in any event within 24 hours of identification of any potential or actual loss to enable the parties to consider what action is required in order to resolve the issue in accordance with the applicable national data protection laws and guidance.

The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of the data security breach in an expeditious and compliant manner.

9. **Training of staff**

It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the information in accordance with the technical and organisational security measures set out in the applicable national data protection laws and guidance.

The level, content and regularity of training shall be proportionate to the staff member’s role, responsibility and frequency with respect to their handling and processing of the information.

**7.10. Storage of shared data**

The recipient of the information is required to keep it securely stored and will dispose of it when no longer necessary. The recipient will not release the information to any third party unless it is fair and lawful to do so. The information will not be transferred outside of the European Economic Area.

**8.11. Individuals rights – Subject Access Requests**

Under the Data Protection Act, individuals can ask to see the information that is held on computer and in some paper records about them. This is called a Subject Access Request (SAR). If individuals wish to know what information is held about them, requests must be put in writing to the organisation processing the data.

**9.12. Review of effectiveness**

This agreement will be reviewed periodically and may be subject to change. On changing the agreement, the new version will be provided on the TPO web site www.tpos.co.uk.
13. Allocation of costs
   Each party shall perform its obligations under this Agreement and resolve any disputes at its own cost.

14. Disputes
   In the event of a dispute or claim brought by a data subject or the Information Commissioner's Office concerning the processing of the information against either or both parties, the parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion.

10.15. Sanctions for Failure to Comply
   Member and Registered Agents are required to co-operate with any investigations by the Ombudsman pursuant to and in accordance with, his Terms of Reference. A failure to share information in accordance with this Agreement may be regarded as a failure to comply with the Ombudsman’s investigations for which sanctions will apply.