Movingworks GDPR Policy

Control Officer : the DCO for Movingworks Limited is Georgina Cox

Movingworks is committed to ensuring that it has adequate controls and provision in place to ensure that the requirements of GDPR are met and the 6 Principles of GDPR are adhered to

1. Personal data must be processed lawfully, fairly and transparently
2. Personal data can only be collected for specific, legitimate and legitimate purposes
3. Personal data must be adequate, relevant and limited to what is necessary for processing
4. Personal data must be accurate and kept up to date
5. Persona l data must be kept in such a form that that the data subject can be identified only as long as is necessary for processing
6. Personal Data must be processed in a manner that secures its security

Processed lawfully, fairly and transparently

Personal data is captured from a range of Movingworks clients;

Sellers and potential sellers

Buyers and potential buyers

Landlords and potential landlords

Tenants and potential tenants

All clients make the first approach to Movingworks either directly or through portals held by 3rd parties such as Rightmove.

Data can only be collected for specific, legitimate and legitimate purposes

There is a need to take and record personal data to comply with legal requirements involved in the process of selling buying and renting property.

There is therefore a legitimate interest of Movingworks as the controller and by 3rd parties used in processing further the information, for example credit checks on tenants and banking details for landlords

Personal data must be adequate, relevant and limited to what is necessary for processing

Sales

Personal details including ID is held for the sellers and purchasers of property. Records are held on the Expert Agent software and on paper files. Records are kept during the sales process and for period of 6 years following the sale.

Potential seller's data is held for 24 rolling months following the initial appointment.

Clients are asked on registration their details if they are happy to be contacted about general marketing, properties and market news. Responses are recorded on EA under "client preferences" which are automatically date stamped.

Rentals

Personal details including ID is held for the sellers and purchasers of property. Records are held on the Expert Agent software and on paper files. Records are kept during the rental process and for period of 6 years following the rental if it is find a tenant only and 6 years from the completion of the managed letting agreement if a managed rental.

Data must be accurate and kept up to date

Whenever contact with clients is made the "last contact "should be updated and the client should always be asked if there have been any changes. Any reported changes must be made instantly Clients have direct access to make themselves inactive through the weekly email or can contact the office by phone email text or post to notify a request. Any such request must be immediately acted on.

Potential buyers and tenants are contacted regularly. Where no contact occurs after 3 months or 3 attempts at contact then the records are permanently deleted.

Data must be processed in a manner that secures its security

Security of Data

Software

All access is password protected and passwords are changed monthly. Access is stripped on staff leaving.

The external software companies (Pay prop; Expert Agent; Home let have confirmed their levels of security which have been deemed secure.

The software provides for automatic destruction of records once a client is marked as inactive.

Hard copies

All paper files are kept under lock and the keys are kept in a locked office. The key to the office is removed form the premises each evening.

Destruction of Data and Documents

Files are archived annually with an external specialist storage company and are destroyed automatically at the 6-year period.

All notes, completed forms for entry on to the software, credit card payment slips and any confidential paperwork is placed in the confidential paper bin as soon as work is completed. The bin is emptied regularly by a specialist firm who provide a certificate of destruction.

Clean desk policy

MW operates a clean desk policy. All desks must be kept clear as much as possible and paperwork must be removed from the desk when leaving the office for any appointments and at the end of the day.

All personal data must be destroyed as soon as it has been entered onto the system by placing it in the confidential waste bin on the 1st floor. No data must be left unattended on desks.

Consent

You must secure clear and unambiguous consent from the data subject to hold their data. And the data subject must consent to each processing activity. EA allows consent to be captured for weekly news letters, general marketing property marketing. All potential purchasers or tenants must be asked if they consent to each of these areas. Where a request is made for details of a specific property rather than a request to go on the "mailing list" always ask if they only want their data taken only for that specific property or are they happy to be contacted about similar properties. If they are there criteria should be taken and only properties matching that criteria must be made available to them using the automated matching process on EA.

Clients must be given the opportunity to withdraw consent and this is noted on all email correspondence.

Third Parties

Our third parties need to provide "sufficient guarantees that they can and will implement appropriate technical and organizational measures" that their processing complies with GDPR and ensures that data subjects rights are protected.

Breaches

If there is a suspected breach the DPO must be consulted with immediately to see if a notification is necessary.

A report must be submitted within 72 hours of becoming aware of the breach

The report must be in a specific format and must describe the measures being taken to address the breach and mitigate side effects.

Data Subject Rights

If infringed the data subject has the right to seek compensation for damages arising from breaches of GDPR

SAR

A Data Subject has the right to request extracts of all personal information that is held about them. The response must be made promptly and must be made within 40 days. The portals are putting steps in place to assist in responding to data subject access requests and Office 365 is used in MW to comply with this for data held outside the software and portals used.

Version 3

11.05.18