DPIA
(Data Protection Impact Assessment)

Step 1: Identify the need for a DPIA

- New Data about individuals will be collected
- Individuals will need to provide information about themselves
- Information will be disclosed to organizations or people who have not previously had access

Step 2: Describe the processing

1. Data will be collect from the customer, rightmove PlC, Onthemarket PLC, Paveys website, mortgage brokers via email, phone, or in person
2. Data will be stored in the form of *digital or hard* copy on secure, password protected servers or in a secure, locked filing cabinet.
3. Data will be used by Paveys employees, maintenance people for the purpose of viewings, contacting clients about the sale of their home, allowing trades people to contact homeowners to arrange access to a property or to inform an individual of Paveys services or offers

Data collected will include Name, Address, Contact information, Photo ID, Mortgage information, Mortgage broker information, and in the case of cash buyers, proof of funds.

Data will be used for contact between the client and Paveys regarding the sale of a property, marketing and offers

Data will be keep for 7 years for clients that have bought and sold a property with us and 12 months for anyone else if there has been no contact.

Data will be used to sell services, arrange viewings/access, agree property sales

Step 3: Consultation process

Consultation is not needed

Step 4: Assess necessity and proportionality

Lawfully, we need to process this information because under money laundering laws we need to know the source of funding for buyers.

We only store data that is needed to complete our business with the client/customer and we take all reasonable measures to ensure it is stored securely including password protected servers, regular backups, locked filing cabinets and software protection

Data is only used in the UK

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Interception of data during transmission (e.g. data sent by email)	Possible	Severe	Low
Physical Access to data stored	Remote	Significant	Low
Software vulnerability such as Malware in the system allowing attacked to steal data or information	Remote	Severe	Medium
Loss of data due to failure to backup or similar incident	Possible	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Interception of data	Data only to be sent and received by well recognised secure email services (Gmail or similar)	Reduced	Low	Yes
Physical Access to data	Limited access to data for employees. All data stored on secure devices or locked filing systems.	Reduced	Low	Yes
Software vulnerability	Software is secured by McAfee anti-virus to ensure maximum security is in place	Reduced	Low	Yes
Data Loss	All data is stored on Microsoft Azure which uses cloud storage and backs up data every day	Eliminated	Low	Yes

Step 7: Sign off

Item	Name/date	Notes
Measures approved by:		Actions and risk reductions all accurate as of date of signature and reviewed every 12 months