

APPENDIX ONE:

IDENTITY VERIFICATION AND FRAUD PREVENTION CHECKS

What we process and share for identity and fraud checks

As well as using your personal information to manage the product or service we have with you, we will also use and share that information about you with fraud prevention agencies including SIRA and National Hunter who will use it to prevent fraud and money-laundering and to verify your identity. This includes by carrying out fraud checks. All this requires us to process your personal information. We will do these checks before we provide the product or service to you, open your account or set up your policy (as relevant) and periodically at other stages after that. If fraud is detected at any time you could be refused the product or service or have it withdrawn from you.

The personal information you have provided, we have collected from you (whether directly or indirectly through our Partners and Brokers), or which has been received from third parties may include your name, date of birth, home address and address history, contact details such as email address, home and mobile telephone numbers, financial information, employment details, device identification including IP and/or MAC address and vehicle details (as relevant and depending on the product or service).

We, and fraud prevention agencies, will use this information to prevent fraud and money laundering, and to verify your identity. We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal information to detect, investigate and prevent crime.

Fraud prevention agencies can hold your personal information for different periods of time, depending on how that data is being used. You can contact them for more information. If you are considered to pose a fraud or money laundering risk, your data can be held by fraud prevention agencies for up to six years from its receipt.

Information on these fraud prevention agencies, including their contact information and information on their Data Protection Officers, can be obtained by contacting dataprotectionofficer@hrbs.co.uk

Automated decisions relating to identity and fraud checks

As part of our processing of your personal information, we may take decisions by automated means. You may automatically be considered to pose a fraud or money laundering risk if our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers, inconsistent with your previous submissions, or if you appear to have deliberately hidden your true identity.

You have rights in relation to automated decision making. There is more detail on this below.

Consequences of processing for identity and fraud checks

As indicated, if we, or a fraud prevention agency, determine(s) that you pose a fraud risk or money laundering risk, we may refuse to provide the product or service to you, open your account or set up your policy (as relevant). If fraud is detected at any time you could be refused the product or service, or have it withdrawn from you. If you would like to know more, you can contact the Data Protection Officer at the Fraud Prevention Agency (for details about what they do) or our Data Protection Officer (for details about what we do) by emailing dataprotectionofficer@hrbs.co.uk

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, you can contact the appropriate fraud prevention agency using the details provided above.

Data transfers for identity and fraud checks

Some fraud prevention agencies may transfer your personal information outside of the European Economic Area. Where they do, they impose contractual obligations on the recipients of that data. Those obligations require the recipient to protect your personal information to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing and where the framework is the means of protection for the personal information.

Lawful processing for identity and fraud checks

When we and fraud prevention agencies process your personal information for the checks described in this section, we do so on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing may also be a contractual requirement in order for us to provide the products and services or to open your account relating to that product.

Your rights in the context of identity and fraud checks

Your personal information is protected by legal rights which include (in the context of the checks described in this section) your rights to object to processing of your personal information, request that your personal information is erased or corrected, or request access to your personal information. If you want to exercise any of these rights, you may contact our Data Protection Officer by emailing dataprotectionofficer@hrbs.co.uk and you can also complain to the Information Commissioner's Office (more details below).