GDPR POLICY

Policy & Principles

This policy will apply to the processing of personal data in manual and electronic copies kept by AMBC Limited.

AMBC Limited is committed to ensuring the personal data, including special categories of personal data and criminal offense data is processed in line with GDPR and domestic laws. If any third-party companies process data on our behalf, then AMBC Limited will ensure that the third-party company takes measures to maintain our commitment to protecting data. We understand that we are accountable for the processing, management and regulation, storage and retention of all personal data held in the form of manual records and on computers.

GDPR applies strict compliance rules and introduces penalties for non-compliance. Penalties could be 4% of the global annual turnover or £20m (whichever is higher). This is a few times higher than the current ones of £500,000 under DPA.

All personal data obtained and held by the company will:

• Be processed fairly, lawfully and in a transparent manner.

• Be collected for specific, explicit and legitimate purposes.

• Be adequate, relevant and limited to what is necessary for the purposes of processing.

• Be kept accurate and up to date. Every effort will be made to ensure that inaccurate data is rectified or erased without delay.

• Must not be kept longer than its given purpose.

• Be processed in a manner that ensures security of personal data.

• Comply with the relevant GDPR procedures for international transferring of personal data.

In addition, the personal data will be processed in recognition of an individual's data protection rights:

• The right to be informed.

• The right to have access.

• The right for any inaccuracies to be corrected.

• The right to have any information deleted.

• The right to restrict the processing of data.

• The right to portability.

• The right to object to the inclusion of any information.

• The right to regulate any automated decision making and profiling of personal data.

AMBC Limited have taken the following steps to ensure that the personal data of individuals are protected:

• Appointed employees to be responsible for the processing and controlling of data, reviewing and auditing of the data protection systems and procedures and overviewing the effectiveness and integrity of all the data that must be protected.

• Provide information to employees on data protection rights, how their data will be used and how it will be protected. Information provided will include the actions they can take if they think their data has been compromised in any way.

• Provide information and training to employees to make them aware of the importance of protecting data, teaching them to protect the data and to understand to treat information confidentially.

• Be accountable for all the personal data we hold, where it comes from, who it is shared with and who it might be shared with.

• Carry out a risk assessment as part of the reviewing process on a regular basis.

• Seek individual's consent for obtaining, recording, using, sharing, storing and retaining personal data. The consent must be freely given, specific, informed and unambiguous.

• Have the appropriate resources in place to detect, report and investigate suspected or actual data breaches. If breaches are made then we have duty of care to report significant breaches to the individual and information commissioner.