Klein
Insurance Management Ltd

167-169 Great Portland Street
London W1W 5PF
Tel: 020 3740 8438

Info@klein-insman.com
www.klein-insman.com

KLEIN INSURANCE MANAGEMENT
DATA PROTECTION POLICY

1. Introduction

This Policy sets out the obligations of Klein Insurance Management Ltd, a company registered in the UK under number 3857258, whose registered office is at The Old Wheel House, 31/37 Church Street, Reigate, Surrey RH2 0AD ("the Company") regarding data protection and the rights of customers and business contacts ("data subjects'") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject'"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

3.1 The right to be informed (Part 12).
3.2 The right of access (Part 13);
3.3 The right to rectification (Part 14);
3.4 The right to erasure (also known as the 'right to be forgotten') (Part 15);
3.5 The right to restrict processing (Part 16);
3.6 The right to data portability (Part 17);
3.7 The right to object (Part 18); and
3.8 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair, and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;
4.2 The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
4.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;
4.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;
4.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
4.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company may collect and process inter alia such personal data as set out in Part 21 of this Policy. This includes:
5.1.1 Personal data collected directly from data subjects.
5.1.2 Personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.

7.2 The accuracy of personal data shall be checked when it is collected and at required intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

9. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

10.1 The Company's Data Protection Officer is Andrew J Hewer, Managing Director.

10.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection related policies, and with the GDPR and other applicable data protection legislation.

10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information.

10.3.1 The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;

10.3.2 The purposes for which the Company collects, holds, and processes personal data;

10.3.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

10.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.3.5 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and

10.3.6 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1 The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

11.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

11.2.1 The type(s) of personal data that will be collected, held, and processed;

11.2.2 The purpose(s) for which personal data is to be used;

11.2.3 The Company's objectives;

11.2.4 How personal data is to be used;

11.2.5 The parties (internal and/or external) who are to be consulted;

11.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

11.2.7 Risks posed to data subjects;

11.2.8 Risks posed both within and to the Company; and

11.2.9 Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Part 12.2 to every data subject:

12.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

12.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided:

12.2.1 Details of the Company including, but not limited to, the identity of its Data Protection Officer;

12.2.2 The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

12.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

12.2.4 Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

12.2.5 Where the personal data is to be transferred to one or more third parties, details of those parties;

12.2.6 Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);

12.2.7 Details of data retention;

12.2.8 Details of the data subject's rights under the GDPR;

12.2.9 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

12.2.10 Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

12.2.11 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

12.2.12 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Customers wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at info@klein-insman.com.

13.3 Responses to SARs shall normally be made within a reasonable period from when such request is received, not exceeding a period of more than two months, however this may be extended by up to three months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Company's Data Protection Officer.

13.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are considered manifestly or unreasonably unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

15.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

15.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

15.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);

15.1.4 The personal data has been processed unlawfully;

15.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Objections to Personal Data Processing

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).

17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

18. Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

Data Ref.	Type of Data	Purpose of Data
Client/Contact Employees	First Name, Last Name, Email Address, Telephone number, Address, Website, Company Information Driving History, Driving Licence Job Title, Passport	Placement of, servicing of, Claims support in respect of, advice in respect of Insurance Contracts arranged or to be arranged on your behalf

19. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

19.1 All emails containing personal data must be sent via the Company's secure servers;

19.2 Personal data may only be transmitted over secure networks;

19.3 Personal data will not accepted in hardcopy form.

19.4 No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from a director.

19.5 All electronic copies will be stored securely on the Company's servers;

20. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

20.1 Personal data must be handled with care at all times and should not be left unattended or on view;

20.2 Computers used to view personal data shall be screen locked before being left unattended;

20.3 All personal data stored electronically should be backed up daily with backups stored offsite;

20.4 All passwords used to protect personal data should be changed regularly and must be secure;

20.5 Under no circumstances will any passwords be written down or shared. If a password is forgotten, it will be reset using the applicable method.

20.6 All software will be kept up-to-date. Security-related updates will be installed as soon as reasonably and practically possible after becoming available;

20.7 No software will be installed on any Company-owned computer or device without approval;

21. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it must be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

22. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

22.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

22.2 Under no circumstances will any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

22.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security related updates; and

22.4 No software may be installed on any Company-owned computer or device without the prior approval of a Director.

23. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

23.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

23.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

23.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

23.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

23.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

23.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

23.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;

23.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

23.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

23.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

23.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1 The Company may from time to time need to transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA in execution of its responsibilities or obligations arising out its role as an insurance broker/advisor.

24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

24.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

24.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

24.2.3 The transfer is made with the informed consent of the relevant data subject(s);

24.2.4 The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
24.2.5 The transfer is necessary for important public interest reasons;
24.2.6 The transfer is necessary for the conduct of legal claims;
24.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
24.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.
25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
25.4 Data breach notifications shall include the following information:
25.4.1 The categories and approximate number of data subjects concerned;
25.4.2 The categories and approximate number of personal data records concerned;
25.4.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
25.4.4 The likely consequences of the breach;
25.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. Implementation of Policy

This Policy shall be deemed effective as of 1st May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

167-169 Great Portland Street
London W1W 5PF
Tel: 020 3740 8438

Info@klein-insman.com
www.klein-insman.com

KLEIN INSURANCE MANAGEMENT
DATA RETENTION POLICY

1. Introduction

This Policy sets out the obligations of Klein Insurance Management Ltd, a company registered in the UK under Company Number 3857258, whose registered office is at The Old Wheel House, 31/37 Church Street, Reigate, Surrey RH2 0AD ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data). In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
b) When the data subject withdraws their consent;
c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
e) When the personal data has to be erased to comply with a legal obligation; or
f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company for the provision of Insurance Broking and Advisory services, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of. For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company for provision of Insurance Broking and Advisory services and by Third Parties such as Insurance Companies and/ or Agent(s) or Broker(s) acting on our behalf with an Insurance Company.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

a) The Company's computers, located in the UK.
b) Third-party servers, operated by Vezo Networks Ltd and located in the UK.
c) Computers permanently located in the Company's premises.
d) Laptop computers and other mobile devices provided by the Company to its employees;

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in Parts 12 and 13 of the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to Parts 22 to 26 of the Company's Data Protection Policy for further details:

a) All emails containing personal data must be sent via the Company's secure servers;
b) Personal data may only be transmitted over secure networks;
c) Personal data will not accepted in hardcopy form.
d) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from a director.
e) All electronic copies will be stored securely on the Company's servers;
f) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation on the part of the Company;
g) Personal data must be handled with care at all times and should not be left unattended or on view;
h) Computers used to view personal data shall be screen locked before being left unattended;
i) All personal data stored electronically should be backed up daily with backups stored offsite;
j) All passwords used to protect personal data should be changed regularly and must be secure;
k) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.
l) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
m) No software may be installed on any Company-owned computer or device without approval; and
n) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of a director to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 27 of the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;
i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;
j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted.
6.2 Personal data stored in hardcopy form shall be shredded and recycled

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:
a) The objectives and requirements of the Company;
b) The type of personal data in question;
c) The purpose(s) for which the data in question is collected, held, and processed;
d) The Company's legal basis for collecting, holding, and processing that data;
e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

8. Roles and Responsibilities

8.1 The Company's Data Protection Officer is Andrew J Hewer, Managing Director.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be responsible for ensuring compliance with the above data retention periods throughout the Company.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 1st May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

167-169 Great Portland Street
London W1W 5PF
Tel: 020 3740 8438

Info@klein-insman.com
www.klein-insman.com

KLEIN INSURANCE MANAGEMENT
PRIVACY POLICY

1. Introduction

Klein Insurance Management Ltd understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of our clients and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

2. Information About Us

Klein Insurance Management Limited

Registered in England:	Company Number 3857258
Registered address:	The Old Wheel House, 31/37 Church Street, Reigate, Surrey RH2 0AD
FCA Registration:	306040
Data Protection Officer:	Andrew J. Hewer
Email address:	info@klein-insman.com
Telephone number:	+44 (0)20 3740 8438
Postal Address:	167-169 Great Portland Street, London W1W 5PF

3. What Does This Notice Cover?

This Privacy Policy explains how we use your personal data: how it is collected, how it is held, and how it is processed. It also explains your rights under the law relating to your personal data.

4. What is Personal Data?

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also extends to less obvious information such as identification numbers. The personal data that we use is set out in Part 5, below.

5. What Are My Rights?

Under the GDPR, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you may contact us to find out more or to ask any questions using the details in Part 11.

b) The right to access the personal data we hold about you. Part 10 will tell you how to do this.
c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 11 to find out more.
d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 11 to find out more.
e) The right to restrict (i.e. prevent) the processing of your personal data.
f) The right to object to us using your personal data for a particular purpose or purposes.
g) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.
h) Rights relating to automated decision-making and profiling. We do not use your personal data in this way

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11. Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau. If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

5. What Personal Data Do You Collect?

We may collect inter alia the following personal data (this may vary according to your relationship with us):

- Name and Date of birth
- Address
- Email address
- Telephone number
- Business name
- Job title
- Driving Licence Number and Driving History (i.e. Accidents & Convictions)
- Copy Passport
- Details of Criminal Convictions

6. How Do You Use My Personal Data?

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for one of the following purposes:

- Providing and managing your contracts of insurance
- Supplying our services to you
- Communicating with you - This may include responding to emails or calls from you.

- Supplying you with information by email (you may unsubscribe or opt out at any time by emailing us at info@klein-insman.com

With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email, telephone or text message with information, news, and offers on our services. You will not be sent any unlawful marketing or spam.

We will always work to fully protect your rights and comply with our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and you will always have the opportunity to opt-out.

7. How Long Will You Keep My Personal Data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

- All Data shall be kept in accordance with our Regulatory obligations as determined by the Financial Conduct Association.

8. How and Where Do You Store or Transfer My Personal Data?

We store or transfer your personal data in the UK. This means that it will be fully protected under the GDPR. We may be required in the performance of our obligations to and/or in the execution of your insurance contracts to transfer personal data outside of the UK to our overseas representatives.

The security of your personal data is essential to us, and to protect your data, we take a number of important measures, including the following:

- All data and drives are held on remote secure servers

9. Do You Share My Personal Data?

We will not share any of your personal data with any third parties for any purposes, except in the following circumstances:-

- In circumstances where we are required to perform our obligations in the execution of your insurance contracts. This may be provided to an Insurance Company or Agent or Broker acting on our behalf with an Insurance Company.

- In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

10. How Can I Access My Personal Data?

Should you wish to know what personal data we hold about you, you may ask us to provide details of this and to provide a copy of such information, where any such personal data is held. This is known as a "subject access request".

All subject access requests must be made in writing and sent to the email or postal address shown in Part 11. There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within a reasonable period from when your request is received, not exceeding a period of more than two months. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. We will keep you informed of our progress.

11. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including a subject access request, please use the following details:

Email address:	info@klein-insman.com
Telephone number:	+44 (0)20 3740 8438
Postal Address:	167-169 Great Portland Street, London W1W 5PF

12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Where any changes are necessary, we will communicate these to you by an accepted method of communication.

Klein
Insurance Management Ltd