Key Health Partnership & Plumstone Corporation Privacy Policy

• Who are we?

Key Health Partnership Ltd is authorised and regulated by the Financial Conduct Authority. Our FCA registered number is 606391. Our Trading Address is Suite 15, Citibase Brighton, 95 Ditchling Road, Brighton, East Sussex, BN1 4ST. Key Health is a trading name of Key Health Partnership Ltd.

Plumstone Corporation Ltd is an authorised representative of Key Health Partnership Ltd. Plumstone Corporation Ltd is registered with the FCA, registration number is 411350.

• Introduction

As of the 25th May 2018, The General Data Protection Regulation (GDPR) became law across the European Union, this also became law in the United Kingdom when we left the EU. These will be the most significant changes to data protection law for 20 years, so we've set out the ways that we intend to comply with these new regulations below.

• Personal information

When providing you with our services, we're likely to require personal information. This is information about you from which you can be identified, for example, your name and contact details. Depending on which services we provide you with, this may also include sensitive personal data such as medical information.

By providing us with your data/information, including engaging with our website (www.keyhealthpartnership.com), you consent to its use as described within our privacy policy. If we make changes to the way we process personal information, this web page will be updated accordingly.

• Confidential medical information

Managing your personal information confidentially and securely is our primary concern and we will comply with GDPR requirements from 25th May 2018.

We are registered at The Information Commissioners Office:

Key Health - Registration Number: Z2414495
Plumstone Corporation - Registration Number: Z7572243

Your confidential medical information will only be disclosed to those involved in providing you with your cover and, if necessary, when sourcing polices on your behalf. This will be done in accordance with UK law.

• Securing your information

Keeping your personal information secure is extremely important to us. We have strong internal procedures in place along with electronic security procedures intended to safeguard and secure the information we collect and retain. All our staff understand that they have a legal duty to respect the confidentiality of your information.

• Telephone call recording

We may record telephone calls for training, quality assurance, complaint handling, evidencing advice given, and to meet our legal and regulatory obligations. Call recordings may contain personal data discussed during calls. Our lawful basis for this processing is our legitimate interests in operating and improving our services and, where applicable, compliance with legal and regulatory requirements. Call recordings are stored securely, and access is restricted to authorised personnel only. Individuals have the right to request access to call recordings that contain their personal data, subject to applicable legal exemptions.

We store our client information on our own CRM, built to our own specifications using the following systems to ensure your security:

Server Protection

- Managed Detection & Response (MDR): 24/7 threat monitoring and rapid incident response to prevent breaches.
- Enterprise-Grade Firewalls (Router): Encrypted network traffic and access controls.

Software Security

- Antivirus & Malware Scans: Regular system scans using industry-trusted tools (e.g., VirusTotal).
- Juggernaut Security: Advanced firewall and intrusion detection for servers.

Website Security

- AIOWPS: Real-time WordPress protection (firewall, login hardening, and spam blocking).
- Malcare: Automated malware removal and vulnerability patching.

We will often send or receive your information by email, and you can find security information from our email facilitator (Send Grid) here:

https://sendgrid.com/resource/general-data-protection regulation/?mkt_tok=eyJpIjoiT1RBd05HUTVabUl4T1RFeSIsInQiOiJpNWlDRVNxbVhOaUZiZGxIZVJlY2g5czBLb0ZObEI3b1lzdTdrdkkwRkZ2MWlvckloY0R1OTRGWDlFSlIIczN3N08zNlBzRDlObnJEWUVJTlpRbzhDVXNwODhjSitRWW4rZ0hlOFZHOUNhNzlUM2Erc2JHSzQrU0xpNnhsODR6aCJ9

We also use an additional CRM leased through HubSpot which uses a multi-layered security approach to protect customer data and support compliance with regulations like UK GDPR. Here are the key measures:

Encryption

- Data in Transit: All data transmitted between your browser and HubSpot servers is encrypted using TLS (Transport Layer Security).

- Data at Rest: HubSpot encrypts stored data using AES-256 encryption, which is an industry standard for strong security.

Access Controls

- Role-Based Permissions: You can assign granular permissions to users based on their role, limiting access to sensitive data.
- Two-Factor Authentication (2FA): Adds an extra layer of security beyond passwords.
- Audit Trails: HubSpot logs changes to contact properties and user actions for compliance and accountability.

Additional Compliance Features

- Consent Management: Built-in tools for adding consent checkboxes on forms and managing lawful bases for processing.
- Cookie Banner: Customizable cookie consent banner for compliance with GDPR and ePrivacy rules.
- Data Subject Rights: HubSpot enables:
- Export of personal data.
- Permanent deletion of contacts.
- Logging of data requests for audit purposes.

Sensitive Data Handling

- HubSpot allows storage of **Sensitive Data** (e.g., financial or health info) under strict controls:
- Requires **Super Admin permissions** to enable.
- Restricted use in certain tools (e.g., personalisation tokens).
- HIPAA support for health-related data when configured properly.

Infrastructure & Monitoring

- HubSpot uses secure cloud infrastructure with redundancy and disaster recovery.

- Continuous security monitoring and vulnerability management.
- Compliance certifications include SOC 2 Type II and ISO 27001.

When using our website, you'll notice a green padlock symbol to indicate that our website is secure meaning that your information will be encrypted as it moves from your computer to our server.

We also process paper documents, mainly provided by the insurers on our client's behalf. Once any such documents are scanned and uploaded to our CRM and/or forwarded to our clients they will be collected and taken away to be securely shredded by Paper Round Ltd, using their 'off-site shredding' service as outlined here: https://www.paper-round.co.uk/service/secure-shredding

• Information we may hold about you

- Identification details such as name, date of birth, address, contact details
- Health related information relating to you and your close relatives, particularly when providing advice on private medical insurance and protection products such as life insurance
- Financial information, particularly when providing advice on group protection products as cover levels are often defined by a multiple of earnings.
- Quotes we've completed on your behalf
- Details of historic policies of which you have been enrolled
- Information about complaints and incidents
- Information that you have provided to enable us to assist you with queries you might have about a claim

• When will we collect information

- When you apply for a quote or policy
- When you enter a contract with an insurer
- When you submit a query to us, for example by email, telephone or social media
- When you participate in any marketing activity
- When you are named in an application form or as a policyholder or dependant
- When we process an application (where we may carry out credit or fraud checks), or when we obtain medical reports on your behalf
- When we liaise with your family, employer, health professional or insurer
- When you engage with us using social media
- For more information about how social networks will manage your data please visit the following pages:

https://en gb.facebook.com/business/gdpr
https://gdpr.x.com/en.html
https://policy.pinterest.com/en-gb/privacy-policy

- When you visit our website by using analytical software to collect information about visitor behaviour. Google Analytics stores information about which pages your visit, how long you are on the site, how you got here and what you click on. You can find more about Google's privacy policy here:
  http://www.google.com/policies/privacy/

• Sharing your personal information

We may share your information between Key Health & Plumstone Corporation for administrative purposes and to provide specialist advice from one organisation to the clients of another and vice versa. This will only occur when we have your prior agreement. The relationship between these three companies is outlined in the 'who are we?' section of this document.

We may share your personal information with insurance companies to obtain quotes, underwriters' guidance and to assist if you have queries about a claim.

To maintain our Anti-Money Laundering obligations, we may use an outside organisation (Lexis Nexis) to help us ensure that our policyholder is who they say they are. The system will check registers including the electoral roll, Tracesmart register (now part of Lexisnexis Risk Solutions) and telephone directories, as well as checking for CCJ's and insolvency along with notifications of company directorships to authenticate the information provided.

You may be enrolled on a policy where another member of your family is the 'main member'. In such instances we'll send all membership documents to the main member. In a situation where we assist in the claiming process, we may also gather medical information and report back to the main member to update them if they seek our assistance on your behalf.

Our service may be provided at the request of your employer, or where the employer of another family member is the policyholder and pays the premium to the insurer. In such cases, we may share your information, in order to administer the policy, with the employer,

the employer's insurer, or the trustees of your scheme. We won't share the details of your medical health or treatment with the employer without your consent to do so.

•Third Party Processors

Our carefully selected partners and service providers may process personal information about you on our behalf as described below

We use an independent outside organisation (Complete Compliance, registered number 07803294) to perform compliance and file checks following the implementation of a new policy.

We use an outside personal assistant Starling Services for copyright, calendar management, preparation and distribute of mailshots, and data processing meaning that they have access to a list of email addresses, telephone numbers, contact names and associated company names, where applicable, but no further information.
We periodically appoint digital marketing agents to conduct marketing activity on our behalf; such activity may result in the compliant processing of personal information. Our appointed data processors include:

• Using your information

We use your personal information to provide you with the following elements of our service:

- Responding to your queries
- Providing you or your employer with a market review
- Completing application forms
- Providing advice and assistance regarding your claim
- Internal record keeping and administration
- Responding to requests where we have a legal or regulatory obligation to do so
- To send you service-related information
- To send promotional material on products, special offers or other information we think you may find interesting (where you have agreed for us to contact you)
- When asking you to complete a customer satisfaction survey

• Storage of your information

We will keep your personal information for as long as is necessary and in accordance with UK law as detailed in our Data Retention Policy . We may retain historical information such as membership documents of facts that relate to cancelled policies as it may be necessary to go back to the terms of a previous policy to ensure future policies were enrolled on the correct terms where a continuation option has been selected. We may also retain information that can be used to outline our advice and to establish your influences when selecting a policy.

• Purpose Limitation & Data Minimisation

- We collect data only for specific, legitimate reasons
- We do not reuse data for unrelated purposes without further consent
- We collect only the data we genuinely need
- We avoid excessive or irrelevant data collection

• Keeping you informed

We will inform you of your renewal information and options annually as your renewal date approaches, this is an essential part of an annual policy renewing and we won't ask for your permission to undertake this process.

We would also like to keep you up to date using mail, email, phone, or text message to inform you of products and services that we think you might be interested in. When we collect your information, we will ask for your permission to allow us to contact you in this way. Your preferences will be obtained by you responding to an email from us or by your verbal agreement. Once your preferences are provided, we will record them on our CRM.

If you do opt in to be contacted about products and services, we will use a system called Mailchimp to deliver our mailshots and your details will only be added to the recipients list once you have opted in. Mailchimp also has an 'opt out of future mailshots' button so, if you change your mind and opt out at a later stage, clicking this will also remove you from the recipients list, you can also see Mailchimp's privacy policy here:

https://mailchim p.com/legal/privacy/?_ga=2.179299489.448831307.1525872408-662195649.1525357155

If you do opt in, we may use your personal information for the following:

- To decide which services to inform you about based on their relevance to you
- To decide which method would be best to use to make contact
- To contact you with details of our services

You can decide that you do not wish to receive marketing information at any time. If you change your mind and would like to stop receiving messages, please contact us using the options below:

• Access to your information

If you have questions regarding your data, you can contact us as follows:

Email us: info@keyhealthpartnership.com
Write to us: Suite 15, Citibase Brighton, 95 Ditchling Road, Brighton, East Sussex, BN1 4ST

You can contact us at the above address should you need to request a copy of the personal information that we hold about you. You may also ask us to remove or correct any information that you believe to be inaccurate. We do not make a charge for providing this information in the first instance however, we may charge a reasonable fee for the administrative costs of complying with the request if it is manifestly unfounded, excessive or if an individual requests further copies of their data following an initial request. We may also ask you to provide proof of your identity along with written consent or proof of your legal right if you require the personal information of another individual.