



## PRIVACY STATEMENT – EU/GDPR REGULATIONS

Property Guardian Protection Limited (“PGP”, “PGPL”, “we,” “us,” “our,” or the “Company”) is committed to protecting the privacy of individuals who visit the Company’s Web sites (“Visitors”), individuals who register to use the Services as defined below (“Customers”), and individuals who register to attend the Company’s corporate events (“Attendees”). This Privacy Statement describes PGP’s privacy practices in relation to the use of the Company’s Web sites and the related services and products offered by PGP (collectively, the “Services”), as well as individuals’ choices regarding use, access and correction of personal information.

In order to provide our services to you we need to collect and process personal information, including financial information about you. For the protection of your data we use physical, technical and organisational measurements. We reserve the right to amend or modify this Privacy Statement at any time and in response to changes in applicable data protection and privacy legislation.

Except as set out in this Privacy Statement, we will not disclose any of your information to other parties without your permission unless we are legally required to do so by, for example, a court order or for the purposes of prevention of fraud or other crime. By submitting information into our website, you consent to the processing of this data about you by us and the product providers

If you have questions or complaints regarding PGP’s Privacy Statement or associated practices, please contact us [info@propertyguardianprotection.com](mailto:info@propertyguardianprotection.com)

### 1. Web sites covered

This Privacy Statement covers the information practices, including how the Company collects, uses, shares and secures the personal information you provide, of Web sites that link to this Privacy Statement (collectively referred to as “Property Guardian Protection Limited’s Web sites” or “the Company’s Web sites”).

PGP’s Web sites may contain links to other Web sites. The information practices or the content of such other Web sites is governed by the privacy statements of such other Web sites. The Company encourages you to review the privacy statements of other Web sites to understand their information practices.

### 2. Information collected

Potential “Customers” (Wanting to be a Guardian):

When expressing an interest in obtaining additional information about the Services, or registering to use the Web sites or other Services, PGP requires you to provide the Company with personal contact information such as name, current address, phone numbers, and email address (“Required Contact Information”), date of birth, nationality and current employment situation



and whether you have a partner that you want to live with and the areas you are interested to live in.

When registering for an event, PGP may also require you to provide the Company with financial information, such as credit card number, (“Billing Information”) and the number of interested parties coming to the event. PGP may also ask you to provide additional information related to the event such as interests that you have which relate to the event etc.

#### Potential “Clients”:

When expressing an interest in obtaining additional information about the Services, or registering to use the Web sites or other Services, or registering for an event, PGP requires you to provide the Company with personal contact information, such as name, company name, address, phone number, and email address (“Required Contact Information”). When purchasing the Services or registering for an event, PGP may also require you to provide the Company with financial qualification and billing information, such as billing name and address, credit card number, and the number of employees within the organization that will be using the Services (“Billing Information”). PGP may also ask you to provide additional information, such as company annual revenues, number of employees, job role, industry and service/event related questions (“Optional Information”).

#### Other Visitors:

When Visitors apply for a job with the Company, PGP may also require you to submit additional personal information as well as a resume or curriculum vitae (“Applicant Information”). Required Contact Information, Billing Information, Applicant Information, Optional Information and any other information you submit to PGP to or through the Services are referred to collectively as “Data.”

As you navigate the Company’s Web sites, PGP may also collect information through the use of commonly-used information-gathering tools, such as cookies and Google Analytics. Google Analytics includes standard information from your Web browser (such as browser type and browser language), your Internet Protocol (“IP”) address, and the actions you take on the Company’s Web sites (such as the Web pages viewed and the links clicked). For additional information about the collection of Google Analytics by PGP, please see page 6 below.

### 3. Use of information collected

The Company uses Data about PGP Customers and Clients to perform the services requested.

For a “Customer” example, if you fill out a “Application form for room” Web form, the Company will use the information provided to contact you about your interest in the Services.

For a “Client” example, if you want to receive a newsletter “Sign up for a Newsletter” Web form, the Company will use the information provided to send you information about what you have selected as your interests.



The Company also uses Data about PGP's Attendees to plan and host corporate events, host online forums and social networks in which event Attendees may participate, and to populate online profiles for Attendees on the Company's Web sites. Additional information on the Company's privacy practices with respect to Data about PGP's Attendees may be found in additional privacy statements on the event Web sites, as the case may be. Please go to the website for more information on bulletin boards, blogs or chat rooms provided by PGP in connection with its corporate events.

The Company may also use Data about PGP's Customers and Clients and Attendees for marketing purposes. For example, the Company may use information you provide to contact you to further discuss your interest in the Services and to send you information regarding the Company, its affiliates, and its partners, such as information about promotions or events. PGP will only do this if you have agreed to this on one of our web forms.

PGP may also receive information about Customers and Clients and Attendees from other sources, including third parties from whom we have purchased data, and combine this information with Data we already have about you. This helps us to update, expand and analyse our records, identify new customers, create more tailored products and services that may be of interest to you

PGP uses Google Analytics to operate and improve the Company's Web sites. The Company may also use Google Analytics alone or in combination with Data about PGP Customers / Clients and Data about PGP's Attendees to provide personalized information about the Company. For additional information about the use of Web Site Navigational Information, please click [here](#).

## 4. Web Site Navigational Information

### Cookies, Web Beacons and IP Addresses

PGP uses commonly-used information-gathering tools, such as cookies and Google Analytics, to collect information as you navigate the Company's Web sites ("Web Site Navigational Information"). As described more fully below, we and our partners use these cookies or similar technologies to analyse trends, administer Web sites and Services, track users' movements around our Web sites and Services, serve targeted advertisements and gather demographic information about our user base as a whole. This section describes the types of Google Analytics used on the Company's Web sites and Services, and how this information may be used.

#### Cookies

PGP uses cookies to make interactions with the Company's Web sites easy and meaningful. When you visit one of the Company's Web sites, PGP's servers send a cookie to your computer or device. Standing alone, cookies do not personally identify you; they merely recognize your Web browser. Unless you choose to identify yourself to PGP, either by responding to a promotional offer, opening an account, or filling out a Web form (such as a "Email Alerts" or a "sign up to a Newsletter" or "Application for a room" Web forms) or have previously identified yourself to PGP, you remain anonymous to the Company.

PGP uses cookies that are session-based and persistent-based. Session cookies exist only during one session. They disappear from your computer or device when you close your browser software



or turn off your computer. Persistent cookies remain on your computer or device after you close your browser or turn off your computer. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our Web sites or Services.

The following sets out how PGP uses different categories of cookies and your options for managing cookies' settings:

| Type of Cookies       | Description   | Managing Settings   |
|-----------------------|---|---|
| Required cookies      | Required cookies enable you to navigate the Company's Web sites and use its features, such as accessing secure areas of the Web sites and using PGP Services. If you have chosen to identify yourself to PGP, the Company may place on your browser cookies containing an encrypted, unique identifier. These cookies allow the Company to uniquely identify you when you are logged into the Web sites and Services and to process your online transactions and requests.  | Because required cookies are essential to operate the Company's Web sites and the Services, there is no option to opt out of these cookies.   |
| Functionality cookies | Functionality cookies allow the Company's Web sites and Services to remember information you have entered or choices you make (such as your username, language, or your region) and provide enhanced, more personal features. These cookies also enable you to optimize your use of PGP's Web sites and Services after logging in. These cookies can also be used to remember changes you have made to text size, fonts and other parts of web pages that you can customize. Functional cookies may also be used to improve how the Company's Web sites and Services function and perform, to enhance and customize your interactions with the Company, and to help us provide you with more relevant messages, including marketing communications. These cookies collect information about how Visitors use our Web sites and Services, including which pages visitors go to most often and if | To manage the use of functionality cookies on this Web site, or to opt out of their use, click "Cookie Preferences" in the footer of this page. Note that opting out may impact the functionality you receive when using PGP's Web sites and Services. To learn more about how to control cookies using your browser settings click here. To learn how to manage privacy and storage settings for Flash cookies click here. |



| Type of Cookies                  | Description   | Managing Settings  |
|----------------------------------|---|--|
|                                  | <p>they receive error messages from certain pages. PGP may use its own technology (under the PGP brand name or an affiliated brand name) or third parties to track and analyse usage and volume statistical information from Visitors, Attendees, and Customers, to provide enhanced interactions and more relevant communications, and to track the performance of the Company's advertisements. PGP and its third-party partners may also utilize HTML5 local storage or Flash cookies for these purposes. Flash cookies and HTML local storage are different from browser cookies because of the amount of, type of, and how data is stored. PGP also uses Flash cookies, to store your preferences or display content based upon what you view on our Web sites and Services to personalize your visit.</p>   |  |
| Targeting or Advertising cookies | <p>PGP sometimes uses cookies delivered by third parties to show you ads for PGP products and services that we think may interest you on any devices you may use and to track the performance of Company advertisements. For example, in these cases, cookies remember information such as which browsers have visited the Company's Web sites. The information provided to third parties does not include personal information, but this information may be re-associated with personal information after the Company receives it. If PGP is using one of its own cookie-related products on our own Website, then a cookie related to ads may appear on our Web site under the PGP or one of our affiliated company's name. PGP also contracts with third-party advertising networks that collect IP addresses and other information from Web beacons (see below) on the Company's Web sites and Services, from</p> | <p>To learn more about these and other advertising networks and your ability to opt out of collection by certain third party, please visit the opt-out pages of the Network Advertising Initiative, here, and the Digital Advertising Alliance, here. To manage the use of targeting or advertising cookies on this Web site, click "Cookie Preferences" in the footer of this page. To learn how to manage privacy and storage settings for Flash cookies click here. Various browsers may offer their own management tools for removing HTML5 local storage.</p> |



| Type of Cookies | Description  | Managing Settings |
|-----------------|--|-------------------|
|                 | <p>emails, and on third-party Web sites. Ad networks follow your online activities over time and across different sites or other online services by collecting Web Site Navigational Information through automated means, including through the use of cookies. These technologies may recognize you across the different devices you use, such as a desktop or laptop computer, smartphone or tablet. Third parties use this information to provide advertisements about products and services tailored to your interests. You may see these advertisements on other Web sites or mobile applications on any of your devices. This process also helps us manage and track the effectiveness of our marketing efforts. Third parties, with whom the Company partners to provide certain features on our Web sites or to display advertising based upon your Web browsing activity, use Flash cookies to collect and store information. Flash cookies are different from browser cookies because of the amount of, type of, and how data is stored.</p> |                   |

### Web Beacons

PGP uses Web beacons alone or in conjunction with cookies to compile information about Customers and Visitors' usage of the Company's Web sites and interaction with emails from the Company. Web beacons are clear electronic images that can recognize certain types of information on your computer, such as cookies, when you viewed a particular Web site or Service tied to the Web beacon, and a description of a Web site or Service tied to the Web beacon. For example, PGP may place Web beacons in marketing emails that notify the Company when you click on a link in the email that directs you to one of the Company's Web sites. PGP uses Web beacons to operate and improve the Company's Web sites, Services and email communications.

### Log Files, IP Addresses, URLs and Other Data

As is true of most Web sites, we gather certain information automatically to analyse trends in the aggregate and administer our Web sites and Services. This information may include your Internet Protocol (IP) address (or the proxy server you use to access the World Wide Web), device and application identification numbers, your location, your browser type, your Internet service provider and/or mobile carrier, the pages and files you viewed, your searches, your operating



system and system configuration information, and date/time stamps associated with your usage. Due to Internet communications standards, when you visit or use the Company's Websites and Services, we automatically receive the URL of the website from which you came and the website to which you go when you leave our Website. This information is used to analyse overall trends, to help us improve our Websites and Services, to track and aggregate non-personal information, and to provide the Websites and Services. For example, PGP uses IP addresses to monitor the regions from which Customers/Clients and Visitors navigate the Company's Web sites. PGP also collects IP addresses from Customers when they log into the Services as part of the Company's "Identity Confirmation" and "IP Range Restrictions" security features.

## Social Media Features and Single Sign-on

The Company's Web sites may use social media features, such as the Facebook "like" button ("Social Media Features"). These features may collect your IP address and which page you are visiting on the Company's Web site, and may set a cookie to enable the feature to function properly. You may be given the option by such Social Media Features to post information about your activities on the Company's Web site to a profile page of yours that is provided by a third party social media network in order to share with others within your network. Social Media Features are either hosted by a third party or hosted directly on the Company's Web site. Your interactions with these features are governed by the privacy policy of the company providing the relevant Social Media Features. PGP also allows you to log in to certain of our Web sites and Services using sign-in services such as Facebook Connect. These services will authenticate your identity and provide you the option to share certain personal information with us such as your name and email address to pre-populate our sign-up form.

## Do Not Track

Currently, various browsers — including Internet Explorer, Firefox, and Safari — offer a "do not track" or "DNT" option that relies on a technology known as a DNT header, which sends a signal to Web sites' visited by the user about the user's browser DNT preference setting. PGP does not currently commit to responding to browsers' DNT signals with respect to the Company's Web sites, in part, because no common industry standard for DNT has been adopted by industry groups, technology companies or regulators, including no consistent standard of interpreting user intent. PGP takes privacy and meaningful choice seriously and will make efforts to continue to monitor developments around DNT browser technology and the implementation of a standard.

## 5. Public forums, refer a contact, and customer testimonials

PGP may provide bulletin boards, blogs, or chat rooms on the Company's Web sites. Any personal information you choose to submit in such a forum may be read, collected, or used by others who visit these forums, and may be used to send you unsolicited messages. PGP is not responsible for the personal information you choose to submit in these forums.

Customers/Clients and Visitors may elect to use the Company's referral program to inform contacts about the Company's Web sites and Services. When using the referral program, the Company requests the contact's name and email address. PGP will automatically send the contact a one-time email inviting him or her to visit the Company's Web sites. PGP does not store this information.



PGP posts a list of Customers/Clients and testimonials on the Company's Web sites that contain information such as Customer names and titles. PGP obtains the consent of each Customer/Client prior to posting any information on such a list or posting testimonials.

## 6. Sharing of information collected

### Service Providers

PGP may share Data about PGP, Visitors, Customers and Attendees with the Company's contracted service providers so that these service providers can provide services on our behalf. These service providers are authorized to use your personal information only as necessary to provide the requested services to us. Without limiting the foregoing, PGP may also share Data about PGP Visitors, Customers and Attendees with the Company's service providers to ensure the quality of information provided, and with third-party social networking and media Web sites, such as Facebook, for marketing and advertising on those Web sites. Unless described in this Privacy Statement, PGP does not share, sell, rent, or trade any information with third parties for their promotional purposes.

### Third Parties

Section 4 of this Privacy Statement, Google Analytics, specifically addresses the information we or third parties collect through cookies and web beacons, and how you can control cookies through your Web browsers. We may also disclose your personal information to any third party with your prior consent.

### Compelled Disclosure

PGP reserves the right to use or disclose information provided if required by law or if the Company reasonably believes that use or disclosure is necessary to protect the Company's rights and/or to comply with a judicial proceeding, court order, or legal process.

## 7. International transfer of information collected

PGP has a development team in India who may use your Data for testing purposes in an isolated IT environment. This environment is not storied electronically in India but in Europe. Our development team in India comply with all the procedures and processed of PGP. No Data is stored in India.

## 8. Communications preferences

PGP offers Visitors, Customers/Clients, and Attendees who provide contact information a means to choose how the Company uses the information provided. You may manage your receipt of marketing and non-transactional communications by clicking on the "unsubscribe" link located on the bottom of the Company's marketing emails. Additionally, you may unsubscribe by contacting us using the information in the "Contact us" section below.

## 9. Correcting and updating your information





PGP may retain your information for a period of time consistent with the original purpose of collection. For instance, we may retain your information during the time in which you have an account (portal functionality) to use our Web sites or Services and for a reasonable period of time afterward. We also may retain your information during the period of time needed for PGP to pursue our legitimate business interests, conduct audits, comply with our legal obligations, resolve disputes and enforce our agreements.

You may request to review, correct, delete or otherwise modify any of the personal information that you have previously provided to us through the Company's Web sites and Services. For other requests to access, correct, modify or delete Your Data, please review the "Contacting Us" section below. Requests to access, change, or delete your information will be addressed within a reasonable timeframe.

## 10. Mobile applications

Without limiting the generality of this Privacy Statement, in addition to information gathered through its Web sites or submitted to its Services, PGP may obtain information through applications ("Mobile Applications") that Customers/Clients or their authorized individuals ("Users") download to, and run on, their mobile devices ("Devices"). Mobile Applications provided by PGP may obtain information from, or access data stored on, Users' Devices to provide services related to the relevant Mobile Application. For example, a Mobile Application may: access a camera on a User's Device to enable the User to upload photographs to the Services; access the call history on a User's Device to enable the User to upload that information to the Services; access calendar information on a User's Device to enable the User to match meeting attendees with contacts submitted by the User to the Services; access the geographic location of a User's Device to enable the User to identify contacts submitted by the User the Services who are nearby; or access contact information on a User's Device to enable the User to sync contact information between the information that is stored on the User's Device and the information that is submitted to the Services. Information obtained to provide Mobile Application services may include information obtained in preparation for anticipated updates to those services. Mobile Applications may transmit information to and from Devices to provide the Mobile Application services.

Mobile Applications may provide PGP with information related to Users' use of the Mobile Application services, information regarding Users' computer systems, and information regarding Users' interaction with Mobile Applications, which PGP may use to provide and improve the Mobile Application services. For example, all actions taken in a Mobile Application may be logged, along with associated information (such as the time of day when each action was taken). PGP may also share anonymous data about these actions with third party providers of analytics services. In addition, if a User downloads a PGP Mobile Application after clicking on a third-party mobile advertisement for the Mobile Application or for PGP, the third-party advertiser may provide PGP with certain information, such as the User's Device identification information, which PGP may use to track the performance of its advertising campaigns.

## 11. Changes to this Privacy Statement



PGP reserves the right to change this Privacy Statement. PGP will provide notification of the material changes to this Privacy Statement through the Company's Web sites at least thirty (30) business days prior to the change taking effect.

## 12. Contacting us

Questions regarding this Privacy Statement or the information practices of the Company's Web sites and Services should be directed to:

[info@propertyguardianprotection.com](mailto:info@propertyguardianprotection.com)

## 13. Data Collection Table

### Guardian Applicant

| Data Type                | Reason why we store the data / how we use the date  | Retention Period After Application |
|--------------------------|---|------------------------------------|
| Name and contact details | To contact Guardian Applicant and send Marketing invitations to view properties that you have not selected, of which PGP believes will suit your search | 12 months                          |
| Date of birth            | Check the age is above 18   | 12 months                          |
| Current Address          | To perform a credit check. This forms part of the vetting criteria to become a guardian.  | 12 months                          |
| Employment status        | This forms part of the vetting criteria to become a guardian.   | 12 months                          |

### Guardian

| Data Type                                      | Reason why we store the data / how we use the date  | Retention Period After Guardian has left |
|--|---|--|
| Name and contact details                       | To contact Guardian Applicant   | 1 year                                   |
| Date of birth                                  | Check the age is above 18   | 1 year                                   |
| Photo ID (e.g. copy of passport) & Nationality | To confirm your identity and check that you are legally allowed to live and work/study in the country. This is part of the Guardian vetting criteria. | 1 year                                   |
| Visa (if needed)                               | To verify that you are legally allowed to live and work/study in the country. This is part of the Guardian vetting criteria.                          | 1 year                                   |
| Current Address                                | To perform a credit check. This forms part of the vetting criteria to become a guardian.  | 1 year                                   |
| Credit check                                   | To see if you have a good history of paying, this is part of the Guardian vetting criteria.   | 1 year                                   |



| Data Type   | Reason why we store the data / how we use the date   | Retention Period After Guardian has left |
|---|--|--|
| If appropriate, Guarantor name & contact information                                    | If the Credit Check comes back w   | 1 year                                   |
| Employment status and details.  | This forms part of the vetting criteria to become a guardian.  | 1 year                                   |
| Bank Details  | Set up payment of accommodation Fee and to pay back Damage Security Payment  | 1 year                                   |
| Next of Kin name & contact information  | In cases of emergencies, were PGP needs to contact a Guardians Next of Kin.  | 1 year                                   |
| Address of previous properties from last 5 years and Employment Details of last 5 years | This forms part of the vetting criteria to become a guardian and this information adheres to the Code of practice: BS 8584:2015 Vacant property protection services. | 1 year                                   |
| Financial information including Invoices, credit history                                | Business need – to manage the payments   | 6 years (HMRC regulations)               |
| Signed Licence Agreement  | Business need - to manage the properties   | 7 years (tax reasons)                    |

### Potential Client

| Data Type                | Reason why we store the data / how we use the date  | Retention Period  |
|--------------------------|---|-------------------|
| Name and contact details | To contact Client Marketing will send you from time to time other information relating to your original request. All communication has an opt-out function. | Until you opt out |
| Work Address             | To send correspondences   | Until you opt out |

### Client

| Data Type                                       | Reason why we store the data / how we use the date | Retention Period After Client has left |
|---|--|--|
| Name and contact details                        | To contact Client Marketing campaigns              | 3 years                                |
| Work Address                                    | To send correspondences                            | 3 years                                |
| Correspondence                                  | Business need - to manage the properties           | 3 years                                |
| Bank Details                                    | Set up payments                                    | 3 years                                |
| Property Details (including inspection reports) |  | 3 years                                |



| Data Type  | Reason why we store the data / how we use the date | Retention Period After Client has left |
|--|--|--|
| Financial information including Invoices, credit history | Business need – to manage the payments             | 6 years (HMRC regulations)             |
| Signed contract (offer letter)                           | Business need - to manage the properties           | 7 years (tax reasons)                  |

### Employee

| Data Type  | Reason why we store the data / how we use the date   | Retention Period After Staff has left |
|--|--|---------------------------------------|
| Name and contact details   | To contact staff   | 7 years                               |
| Date of birth  | Check the age is above 18  | 7 years                               |
| Photo ID (e.g. copy of passport) & Nationality   | To confirm your identity and check that you are legally allowed to live and work/study in the country. This is part of the Staff vetting criteria. | 7 years                               |
| National Insurance Number  | To confirm your identity and to set up wage payment.   | 7 years                               |
| Visa (if needed)   | To verify that you are legally allowed to live and work/study in the country. This is part of the Staff vetting criteria.                          | 7 years                               |
| Current Address  | To perform a credit check. This forms part of the staff vetting criteria.  | 7 years                               |
| Credit check 5 years history verification<br>CRB Check Driving Licence 2 Character<br>References Criminal & Civil Records 2<br>Proofs of Address (Utility Bill & Bank Statement) | To perform screening process as specified in BS 7858-2012 - staff screening.   | 7 years                               |
| Bank Details   | To pay wages   | 7 years                               |
| Next of Kin name & contact information   | In cases of emergencies, were PGP needs to contact a employees Next of Kin.  | 7 years                               |
| Wages (payroll) + Bonuses + Pension + Expense Information  | Business need – verifying payment made By Law - HMRC regulations   | 6 years                               |
| Appraisals / Performance Review / Disciplinary History   | Business need – verifying and tracking performance and development   | 7 years                               |
| Attendance records: Absences + Maternity / paternity   | Business need – verifying performance By Law   | 4 years                               |
| Personal accident/injury claim   | Business need – preventing further accident/injury By Law  | 11 years                              |



| <b>Data Type</b>    | <b>Reason why we store the data / how we use the date</b>              | <b>Retention Period After Staff has left</b> |
|---------------------|--|--|
| Training records    | Business need – verifying training needs (performance and development) | 5 years                                      |
| Employment contract | Business need – verifying terms of employment                          | 2 years                                      |

### Employee Applicant

| <b>Data Type</b>                               | <b>Reason why we store the data / how we use the date</b>  | <b>Retention Period</b> |
|--|--|-------------------------|
| Name and contact details                       | To contact staff   | 1 year                  |
| Date of birth                                  | Check the age is above 18  | 1 year                  |
| Photo ID (e.g. copy of passport) & Nationality | To confirm your identity and check that you are legally allowed to live and work/study in the country. This is part of the Staff vetting criteria. | 1 year                  |
| National Insurance Number                      | To confirm your identity   | 1 year                  |
| Visa (if needed)                               | To verify that you are legally allowed to live and work/study in the country. This is part of the Staff vetting criteria.                          | 1 year                  |
| CV   | Business need – investigating suitability for role / verifying experience  | 1 year                  |

### Supplier

| <b>Data Type</b>   | <b>Reason why we store the data / how we use the date</b> | <b>Retention Period After Supplier has delivered product or service</b> |
|--|---|---|
| Name and contact details                                 | To contact Supplier Applicant                             | 1 year  |
| Financial information including Invoices, credit history | Business need – to manage the payments                    | 6 years (HMRC regulations)  |