

Candidate Information Notice

Dear Applicant,

Information Notice – Processing of Personal Data

This Candidate Information Notice is designed to help you understand how Park Place Technologies (Park Place Technologies LLC, 747 Alpha Drive, Cleveland, OH 44123, USA) and all our affiliates (collectively “Park Place Technologies”, “us”, “we”) collect, use and share personal data when you submit an application for employment at Park Place Technologies.

Park Place Technologies is committed to protecting the privacy of individuals applying to positions within Park Place Technologies and its affiliates, and will do everything in its power to ensure that the use of those individuals’ information is carried out with due respect to their fundamental rights and freedoms, as well as their personal dignity, particularly in light of existing obligations on confidentiality and the processing of personal data. We require applicants to provide certain personal information and details in order for these applications to be considered, and we would therefore like to explain the procedures and ways in which we handle data supplied to us.

As such, this Information Notice has been written, in order to allow you to understand Park Place Technologies’ policy regarding your privacy, and how your personal information will be handled when applying to positions at Park Place Technologies.

In general, any information and data which you provide to Park Place Technologies, or which is otherwise provided to Park Place Technologies by recruitment agencies or similar third parties, will be used by Park Place Technologies in compliance with the internationally recognised principles of lawfulness, fairness, transparency, purpose limitation, storage limitation, data minimisation, accuracy, integrity and confidentiality.

Data Controller

The Data Controller regarding all processing operations carried out regarding personal data related to job applicants is the relevant **Park Place Technologies** affiliate you are submitting your application to.

For any questions regarding the processing of Personal Data by Park Place Technologies, please contact: dataprivacy@parkplacetechnologies.com.

Data Protection Officer

European Union: Park Place Technologies has appointed a Data Protection Officer (DPO) for the processing of personal data subject to Regulation (EU) 2016/679 (“GDPR”). The DPO may be contacted for matters relating to such processing:

- at dataprivacy@parkplacetechnologies.com; or
- in Germany, at mail@planit.legal.

Malaysia: If you are based in Malaysia, you may also contact the local DPO at: dpo_parkplacetechnologies@hhq.com.my.

Personal Data Processed

Park Place Technologies may collect information on you, as a job applicant, when you apply directly to a position at Park Place Technologies (e.g., through our website, by e-mail, in person), or when recruitment agencies (and other similar third parties) provide this information to Park Place Technologies, as requested by you.

This information is related to you as an individual and allows you to be identified (either directly, or together with additional information), which therefore classifies it as personal data (“**Personal Data**”).

Personal Data which may be processed by Park Place Technologies, related to recruitment processes, are as follows:

Name, Contact Details and other Personal Data

When you apply to a position at Park Place Technologies, we will collect information on you, such as your name, address and contact details (e-mail address, telephone number, mailing address – including proof of address), date of birth and gender, as well as information included in your cover letter, CV and/or résumé, including details on your previous work experiences, salaries and allowances, academic and professional qualifications, references, records of qualifications, information about professional memberships, portfolios, photographs, passport/driving license/official identification document details and other information collected or generated during the recruitment process, such as interview notes, right-to-work documentation and records or results of pre-employment checks, where applicable.

We may also collect this information from third parties (such as recruitment agencies) where you apply to a position at Park Place Technologies through those third parties' services.

Additionally, we may collect and process Personal Data disclosed in applicants' public professional social media profiles (e.g., LinkedIn), whenever we consider this necessary and relevant to the performance of the job being applied for.

Sensitive Data

CVs, résumés and cover letters, as well as other documents you may upload or provide to us, may contain Personal Data – in particular, they may disclose (inadvertently or not) sensitive Personal Data, such as (but not limited to) information revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation ("**Sensitive Data**").

We ask that you do not disclose any such Personal Data in these documents, or by any other means when applying to a position at Park Place Technologies. If you do so, then we will disregard this Personal Data and, whenever technically feasible, delete it without undue delay.

Without prejudice to the above, we may ask you to provide certain categories of Sensitive Data (racial or ethnic origin, religious or philosophical beliefs, sexual orientation), for the purpose of monitoring equal opportunities provided to applicants, as permitted or required under applicable laws. These Sensitive Data will be anonymised / aggregated as soon as possible after their collection, to allow us to generate non-individual statistics on applicants which we consider for a position at Park Place Technologies.

Separately, where you are required to attend one of our secure sites during the interview process, we may process your biometric data, such as fingerprint data, for the purpose of managing your access to such secure sites, where permitted under applicable laws.

It is **optional** for you to provide all of the Sensitive Data described in this section, and you will suffer no detriment should you choose not to. Where you choose to do so, we will process them based on your explicit consent. You are free to refuse or withdraw such consent at any time, without suffering any adverse consequences (including regarding your application). If you specifically refuse to provide consent for the processing of biometric data where relevant, or later withdraw it, we will make an adequate alternative access procedure available to you where needed.

Any Sensitive Data that you may choose to provide will not be used to discriminate you based on protected characteristics, such as your race, national or ethnic origin, sex, religion, disability or genetic information.

Other Persons' Personal Data

CVs, résumés and cover letters, as well as other documents you may provide to us may also (inadvertently or not) include Personal Data related to other persons. Additionally, you may provide Personal Data related to other persons when including information as to your professional references.

In any situation where you decide to share Personal Data related to other persons, you will be considered as an independent data controller regarding those Personal Data, and must assume all inherent legal obligations and responsibilities. You must ensure that you are lawfully entitled to disclose these Personal Data to us (e.g., because you have those other persons' consent to do so).



Please note that, where you disclose Personal Data related to other persons beyond your lawful entitlement to do so, you must fully indemnify us against any complaints, claims or demands for compensation for damages which may arise from the processing of those Personal Data, initiated by the third parties whose information we process following your initiative.

Purpose of the Processing

The main purpose for which we intend to use your Personal Data is to enable you to submit a job application and to manage such applications, for possible recruitment to positions at Park Place Technologies. This includes, where applicable, communicating with you during the recruitment process, assessing your suitability for the role, conducting interviews and assessments, verifying your right to work, carrying out pre-employment checks, including reference checks, and making offers or preparing employment or engagement documentation.

We may also process your Personal Data:

- in accordance with legal or regulatory requirements which may be applicable to us, such as to respond to subpoenas or requests from government authorities;
- where necessary for us to establish, exercise or defend legal claims, or otherwise to protect our, your or others' rights;
- for the purpose of monitoring equal opportunities provided to applicants, as permitted or required under applicable laws; and
- to protect, investigate and deter against violation of the law, violation of your agreements with us, or otherwise fraudulent, harmful, unauthorized or unethical activity.

Legal Grounds and Mandatory / Discretionary Nature of the Processing

We will generally process your Personal Data, for the abovementioned purposes, due to this being necessary in order to potentially enter into an employment or similar agreement with you, including to receive and assess your application, communicate with you during the recruitment process, conduct interviews and assessments, verify your right to work, carry out pre-employment checks, and make offers or prepare employment or engagement documentation, where applicable.

We will specifically rely on our legitimate interests as a data controller, when processing your Personal Data:

- in connection with assessments we carry out of the professional social media profiles of candidates applying for certain jobs, when this is necessary and relevant for the performance of those jobs: our interest in these assessments is to ensure that the candidate has the appropriate qualifications, professional background and competence to perform the tasks applied for;
- to establish, exercise or defend legal claims;
- to protect rights;
- to monitor equal opportunities provided to applicants (where not required to do so under applicable laws); and
- to protect, investigate and deter against violation of the law, violation of your agreements with us, or otherwise fraudulent, harmful, unauthorized or unethical activity.

Where we are subject to a legal or regulatory requirement to process your Personal Data, the need to comply with that legal or regulatory requirement will be relied on for that processing.

It is not mandatory for you to provide your Personal Data to us for any of the purposes disclosed in this Privacy Notice; however, if you do not, we will not be able to manage any applications you submit to us.

Additionally, please note that you are not required to provide any Sensitive Data to us (as mentioned in the "Sensitive Data" section, above). Should you nonetheless disclose any Sensitive Data, we will not take such information into account when assessing your application and will delete it as soon as technically feasible. Notably, we do not use any disclosed information on existing health or medical conditions, or any genetic information, to carry out hiring decisions. We will only ever request that you provide Sensitive Data in



exceptional cases, clearly indicating the purpose and the legal basis for its use (as also mentioned in the “Sensitive Data” section, above).

Where we ask you to provide Sensitive Data for equal opportunities monitoring, this will be optional and, where required, based on your explicit consent, unless another legal basis is available under applicable law.

Where we process your biometric data, such as fingerprint data, for the purpose of managing access to secure sites during the interview process, such processing will be carried out only where permitted under applicable laws and on the basis of your explicit consent. You may refuse or withdraw your consent without adverse consequences for your application, and we will make available an alternative access procedure where required. We do not knowingly collect Personal Data related to children under the age of 13 (for residents within the European Union) or under the age of 16 (for residents within the United States).

Recipients of Personal Data

We do not sell your personal information; however, we may share your personal information with third parties for a number of reasons. Specifically, your Personal Data may be shared, for the purposes listed in the “*Purpose of the Processing*” section, with the following persons / entities (hereinafter, the “**Recipients**”):

- People, companies or firms that provide us with advice and consultancy concerning accounting, administrative, legal, tax, financial and debt collection matters related to recruitment, including recruitment agencies;
- Entities that help us carry out our processing activities, such as recruitment platform providers and HR/recruitment software providers, website hosting providers, website management providers and data storage providers;
- People we authorise to process Personal Data in order to perform activities that are related to the management of recruitment processes, like our employees. These people are under binding confidentiality obligations (either legal or contractual).
- Other companies within the Park Place Technologies Group, including related organizations, which may be interested in your application;
- Third parties, in connection with a business deal (or potential business deal) such as a merger, consolidation, acquisition, reorganization or sale of assets, or in the event of bankruptcy;
- Public entities, bodies or authorities, when strictly required by law (such as local tax, customs, national security, or law enforcement authorities).

Unless otherwise indicated at the time we collect your personal data, if we allow third parties to access such personal data, we will have contractual provisions or other appropriate protections in place to ensure such access is for limited purposes and in compliance with this Privacy Notice.

Cross-border Transfers of Personal Data

Since we are a global Group with presence in many countries, your personal data may be transferred to recipients in multiple countries. We genuinely care about your privacy and for that reason we have implemented appropriate safeguards to protect your information when it is transferred. Some of these safeguards include adequacy decisions of the European Commission or by the competent UK authorities, standard data protection clauses adopted by the European Commission or by the competent UK authorities, or other safeguards or conditions that are considered adequate to the relative transfer of data under the applicable legislation.

Security

The security of your Personal Data is important to us. We take a number of organizational, technical and physical measures that are designed to protect the Personal Data we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the absolute security of your Personal Data.

Retention of Personal Data

Please see information on the retention periods we apply to the personal information processed within the scope of this Privacy Notice below. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal

information and whether we can achieve those purposes through other means, and the applicable legal requirements.

When you begin submitting an application for a position at Park Place Technologies, the recruitment portal will save your draft application, and any Personal Data within, for up to 2 years (meaning you can leave an application incomplete, and return to it later). Any information contained in your draft application will not be visible to us until you have completed your submission.

After you have submitted an application, we will store the submitted Personal Data, together with your account, for up to 6 months from when we receive them or from the most recent modification or update you make to any submitted Personal Data. After this period, we will destroy your Personal Data.

If, at the end of the abovementioned periods, we believe we may still have an interest in retaining your application and Personal Data further (for example, in order to consider you for future job openings), we will reach out to you, using the contact details you have provided, in order to ask for your consent to hold on to your Personal Data for longer (up to 6 months). You are, naturally, free to refuse this consent or withdraw it at any time (see the “*Data Subject’s Rights*” section, below).

Where we process biometric data, such as fingerprint data, we will retain such data only for the time strictly necessary to manage your access to secured sites and will delete it as soon as it is no longer necessary for that purpose – in particular, as soon as you have left the relevant secure site – unless we are required to retain it for longer under applicable law.

We will keep Personal Data we process in order to comply with legal or regulatory requirements for the period set out in the legal or regulatory obligation.

Where your application is successful, we may retain and further process Personal Data that are necessary for the establishment and management of your employment or engagement relationship. You will receive further privacy information in this respect during the onboarding process.

Data Subjects’ Rights

As a data subject, depending on the laws applicable to you, you may be entitled to exercise all or some of the following rights:

- Access your Personal Data that we are processing (or receive a copy of that Personal Data) and obtain further information about such processing;
- Correct or modify your Personal Data that we are processing when it is inaccurate or incomplete;
- Request that we erase your Personal Data that we are processing, when you feel that the processing is unnecessary or unlawful;
- Request restriction of the processing of your Personal Data, when you feel that the Personal Data we have on you is inaccurate, unnecessary or has been unlawfully processed, or when you have previously objected to its processing;
- Exercise your right to portability: the right to (1) obtain a copy of the Personal Data you have provided to us and which we process based on your consent or a contract we have with you, in a structured, commonly used and machine-readable format, and/or (2) transmit those Personal Data to another data controller;
- Object to the processing of your Personal Data, based on relevant grounds related to your particular situation, which you believe must prevent us from processing your Personal Data; or
- Withdraw your consent to processing, or otherwise opt-out of processing (where applicable).

Where applicable, you can exercise any of the rights mentioned above, as well as the right to otherwise opt-out of the processing of your personal data, by sending a written request, yourself or through an authorized agent, to: dataprivacy@parkplacetech.com, or, if you are based in Malaysia, to: dpo_parkplacetechnologies@hhq.com.my. Please ensure requests are described with sufficient detail so we can properly respond to them, including by specifying which right(s) you are exercising and providing your name, e-mail and scope of your request.



We will respond to privacy requests within the time permitted by applicable law, making an effort to respond promptly, and may require reasonable additional information to verify a request made by you and/or your agent (e.g., name and e-mail address to confirm your identity). If we decline your request, we will tell you why, subject to legal restrictions. We will not discriminate against you for asserting your privacy rights.

As a data subject, you are entitled to file a complaint with the competent supervisory authorities for the protection of personal data, if you believe that the processing of your personal data carried out by us is unlawful. If you are based in the European Union, you can find your relevant supervisory authority here.

We adhere to the EU-U.S. Data Privacy Framework and UK Extension (“DPF”) and commit to subject to DPF Principles applicable data. See <https://www.dataprivacyframework.gov/>. Under the DPF, we may be subject to U.S. statutory bodies and may remain responsible for data shared with third parties. Under certain conditions, the DPF provides the right to invoke binding arbitration and to resolve complaints not resolved by other means.

Amendments

We reserve the right to partly or fully amend this Privacy Notice, or simply to update its content, for example, as a result of changes in applicable law. We will inform you of any changes we deem important, through the available channel(s) we deem most reasonable in light of the context of the specific change, once they are introduced (by sending out an e-mail to the contacts on our mailing lists, and by temporarily adding a pop-up banner to our website), and they will be binding upon us as soon as they are published on our website.

Location-Specific Disclosures

The law requires that we provide additional disclosures to residents of certain countries, regions and states. Please see below for disclosures that may be applicable to you.

Notice to California Residents

If you are a California resident, this section applies to you in addition to the rest of this Candidate Information Notice. This section does not cover information we collect about you as an employee. For more information about our privacy practices relating to employee information, please see our Employee Handbook.

Personal Information We Collect. We collect your personal information when you interact with our website to apply for a position at Park Place Technologies. In the past 12 months, we have collected the following categories of personal information and have used that information for the following purposes:

Category of Personal Information Collected	Business Purpose of Collection	Source(s) of Information
Identifiers, including real name, postal address, online identifier, Internet Protocol address, email address, telephone numbers.	If you choose to disclose this information, we may collect it as part of our employment application process	Directly from you when you contact us or apply for employment with us We also collect your IP address passively from you when you visit and navigate our Site, click on advertisements, or receive or interact with our communications.
Characteristics of protected classifications under California or federal law, including age or date of birth, race, color, national origin, military/veteran status, physical disabilities, mental disabilities, medical condition, gender and gender identity	If you choose to disclose this information, we collect it as part of our employment application process We also collect gender identity to assist in relationship management and ensuring we properly address individuals in our communications (e.g., whether to call someone Ms., Mrs., Mr., etc.)	Directly from you when you apply for employment with us

Occupation, professional, or employment-related information	To communicate with you If you choose to disclose this information, we collect it as part of our employment application process	Directly from you when you set up an account, order or pay for services, or apply for employment with us
Education information	If you choose to disclose this information, we collect it as part of our employment application process	Directly from you when you apply for employment with us

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible business purposes without providing you notice.

Retaining Your Information. We will only keep your personal information in an accessible form which can identify you for as long as we need to for the purposes for which it was collected. Because retention periods vary depending on the purpose for collection, we use certain categories and criteria to determine how long we keep personal information, as further described below. Where your personal information is used for more than one purpose, we will retain your Information for the longer of those periods.

Type of Personal Information	Retention Period
Personal information processed in connection with your employment application	Unsuccessful applicants – 6 months after the date of notification that application has not been successful, unless: (a) otherwise required by applicable law; (b) you consent to us storing it for longer (for example to consider you for future roles); or (c) there is a dispute or other legitimate reason that requires it to be kept for longer. Hired applicants – Please see our Employee Handbook for details.

When we no longer require your personal information, we will take steps to delete or anonymize it. If the information cannot be permanently deleted or anonymized (for example when it is stored in our electronic backups), we will take appropriate steps to ensure that it is: (a) not used in connection with any decision involving you; (b) not shared with anyone except when we are legally required to do so; (c) kept secure; and (d) permanently deleted once possible.

Sharing Your Information. We do not sell your personal information but may disclose some of your personal information to third parties for business and commercial purposes, including sharing certain personal information for cross-context behavioral advertising purposes. In the past 12 months, we have disclosed the following categories of personal information to certain third-party subcontractors and service providers for a business purpose:

Category of Personal Information Disclosed	Category of Third Parties with Whom Information is Disclosed	Purpose for Disclosure
The following characteristics of protected classifications under California or federal law: age or date of birth, race, color, national origin, military/veteran status, physical disabilities, mental disabilities, medical condition, gender and gender identity	Our employment and hiring service providers	To consider you for a position within our organization
Occupation, professional, or employment-related information	Our employment and hiring service providers	To consider you for a position within our organization

Education information	Our employment and hiring service providers	To consider you for a position within our organization
-----------------------	---	--

Sensitive Personal Information. We do not use or disclose sensitive personal information except as necessary to provide you with our services, consider you for employment opportunities, and prevent fraud.

Personal Information of Children. We have no actual knowledge that we sell or share personal information of consumers under 16 years of age.

Your Rights. California residents have certain rights regarding their personal information:

- ***Right to Know.*** You may request no more than twice in a 12-month period that we provide you with copies of specific personal information we have collected, sold, or disclosed about you. However, under California law, we cannot provide you with certain sensitive information, despite your request (for example, we will not send you copies of your social security number even if it is something we collected).
- ***Right to Delete.*** You may request that we delete certain personal information we have collected about you, with certain exceptions.
- ***Right to Correct.*** You may request that we correct inaccurate personal information that we maintain about you.
- ***Right to Opt Out.*** You may opt out of the sharing of your personal information to third parties for cross-context behavioral advertising purposes.
- ***Shine the Light.*** Under California’s “Shine the Light” law, you have the right to ask us once a year if we have shared your personal information with third parties for direct marketing purposes.

Exercising Your Rights to Know, Delete, Correct, or Shine the Light. To exercise your rights above, please submit a request to by filling out our request form found [here](#), by emailing us at dataprivacy@parkplacetech.com or by calling us at 1 (800) 343 4654. Please describe your request with sufficient detail so we can properly respond to your request. As part of your request, please specify which right you are exercising and be prepared to provide your name, email, account name/agreement number, if applicable. We may ask for additional information to verify your identity. The information you provide in your request and any follow-up information we ask for from you will be used solely to verify your request. Only you or an individual designated as your authorized agent to act on your behalf may make a request related to your personal information. We may ask for additional information from you or an authorized agent to verify the agent’s identity and their authority to act on your behalf. After receiving your request, we may need to contact you or your agent for further information and will notify you or your agent if your request has been granted or declined, or if an exception applies to your request. We will not discriminate against you if you choose to exercise your rights.

Responding to Your Rights Request. We will try to respond to your request within 45 days. If we need more time, we will contact you with the reason we need more time and the extension period. We will deliver our written response by mail or electronically, at your option. In response to your request to know, we will only disclose the information we have collected in the 12 months prior to our receipt of your request. Our response will also explain the reasons we cannot comply with any request, if applicable. We do not charge a fee to process or respond to your request unless your request is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate prior to completing your request.

If you have any questions or concerns about our privacy practices or information practices, please contact us at dataprivacy@parkplacetech.com.

Notice to Colorado, Connecticut, Utah and Virginia Residents

We do not process your personal information for the purposes of profiling in furtherance of decisions that produce legal or similarly significant effects concerning consumers. We do not collect sensitive data about you or make sensitive data inferences. If we do so in the future, we will obtain your consent before doing so and we



will provide you with more details about the purposes of processing and data retention periods with respect to any sensitive data at the time of collection. We will only retain your information as long as it is reasonably necessary for the purposes for which it was processed.

If you have submitted a rights request as described in the *Your Rights* section above, we will try to respond to your request within 45 days. If we need more time, we will contact you with the reason and the extension period. We will respond to your request by mail or electronically, at your option, and will notify you if your request has been granted or declined, if an exception applies to your request, any reason we cannot comply with your request, or if we need additional information. We will not discriminate against you if you choose to exercise your rights hereunder. You have the right to appeal our refusal to take action on a rights request within 30 days after receiving our decision by contacting us at dataprivacy@parkplacetechnology.com. We will try to inform you of our decision in writing within 60 days after receipt of your appeal, with a written explanation of our decision. The information you provide in your request and any follow-up information we ask for will be used solely to verify your request and will be deleted as soon as practical after processing your request. We will not charge a fee to process or respond to your request unless your request is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate prior to completing your request.

Notice to Nevada Residents

Nevada law gives Nevada consumers the right to request that a company not sell their personal information for monetary consideration to certain other parties. We do not sell your personal information for monetary consideration; however, this right still applies. If you are a Nevada consumer and wish to exercise this right, please submit your request by contacting us at dataprivacy@parkplacetechnology.com.