Visitor Information Notice

If you are reading this document, it is because you are entering or have entered one of our premises.

We are Park Place Technologies, the data controller, and this Information Notice will help you better understand what data is collected, for what purposes and how you can manage your Personal Data.

If you have any questions about this Information Notice or how your Personal Data is handled by us, you can send us an e-mail at: dataprivacy@parkplacetech.com.

1) What data we process

Depending on how you access our premises, we may collect all or some of the following information.

a) Data you provide for access

When you enter our premises, we may ask you for Personal Data such as your first name, last name, valid identification document (e.g., identity card or passport), company you belong to, time of entry, and exit as well as the Park Place Technologies contact person who accompanies you or whom you came to meet. This collection takes place during your registration as a guest at the entrance and is used to assign you an identification badge to access and register your access to the areas of our facilities.

b) Data collected by the video surveillance system

All entrances to our premises have cameras operating 24 hours a day, seven days a week, including public holidays, in such a way as to limit the visual angle of the entrance area. These cameras are placed to protect individuals and assets inside Park Place Technologies premises and are adequately marked by signs indicating their presence before you enter their cone of visibility.

Through these cameras we are also able to collect other Personal Data such as the number plates of vehicles accessing our premises, as applicable.

c) Sensitive Data provided by you

In some cases, you may provide us with Sensitive Data relating to you or third parties, such as details on mobility disabilities to facilitate access or visits to our premises. It is not our intention to request or use this information unless you believe it is necessary to facilitate your or the third party's access. Otherwise, please do not provide such information to us.

d) Data collected by third parties

Some of your Personal Data may have been provided to us by third parties (e.g., our employees and contractors) with whom you have arranged your visit.

For ease of reading, in the following we will collectively refer to all Personal Data mentioned so far as "Data".

2) Why we use your Data

We use your Data for the following purposes:

a) Accessing and protecting our premises

We use your Data to identify you and register your access to our premises, as well as for the purposes of work safety and protection of company assets, i.e., the protection of people and property against possible aggression, accidents at work, theft, robbery, damage, vandalism to protect people and/or property, and to verify the presence of visitors.

This processing is based on our legitimate interest in protecting persons and assets within our premises, which we have assessed not to be intrusive to your rights and freedoms.

b) Fulfilling legal obligations to which we are subject

We use your Data to comply with our legal obligations (e.g., security legislation). Such processing includes the retention of your Data and the possible communication of your Data to the competent authorities that lawfully request them from us.

Please note that providing your Data for the above purposes a) and b) is not mandatory, but without it, we will not be able to carry out the purposes indicated above, including allowing you to access our premises.

3) How we use your Data

All Data collected for the above purposes is processed both manually and electronically. Your Data may also be subject to combination and/or cross-referencing. This allows us, for example, to combine the "Data you provide for access" with the "Data collected by the video surveillance system" or with the "Data collected by third parties" even before and after your entry.

4) With whom we share your Data

We share your Data with the following categories of entities ("**Recipients**"):

- our authorized persons: these include our employees and contractors who have signed a confidentiality agreement and follow specific rules for the processing of your Data, as well as specific individuals of related entities (e.g., in the event of a sale or merger).

- our data processors: these are the external parties to whom we entrust certain processing operations. For example, this category includes suppliers of the video-surveillance and access control systems implemented in our facilities. We have signed a contract with our data processors to ensure that your Data is processed in accordance with appropriate measures and only based on our instructions.

- law enforcement agencies or any other authority whose orders are binding for us: this is the case, for example, when we have to comply with a court order, a law, a lawful request (e.g., national security requirements), or when it is necessary to defend ourselves in court.

We do not "sell" or "share" any of your Data (outlined herein) for cross-context advertising purposes.

5) Where is your Data

We are present and offer our services globally. We assure you that your Data is processed by us and by the Recipients in accordance with the different data protection laws to which we are subject. For example, transfers of your Data from within the European Economic Area to Recipients outside the European Economic Area may be based on Standard Contractual Clauses approved by the European Commission, or on Park Place Technologies' self-certification under the EU-U.S. Data Privacy Framework. More information on this is available by sending an e-mail to us at: dataprivacy@parkplacetech.com.

6) How long we keep your Data

Data provided by you upon accessing our premises is kept for 120 days after your last visit.

If shared, "Sensitive Data provided by you" will only be kept for the duration of your visit, without being recorded within our systems.

The "Data collected by the video surveillance system" will be retained for 30 days. After this period, video-surveillance footage will be automatically deleted, except in the event that we need to extract footage to defend ourselves, bring a claim in court, or comply with a specific investigative request of a judicial or public security authority.

More information on retention periods is available by sending an e-mail to us at: dataprivacy@parkplacetech.com.

7) Data subjects' (your) 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 Data: we will provide you with the Data we hold about you and where applicable the source of your Data.

- rectify your Data: for example, you may ask us to change the Data you have provided us to enter our premises (e.g., first name, last name, company you work for, etc.) if they are incorrect or out of date.

- limit the processing of your Data: for example, if you believe that processing by us is unlawful and/or you believe that certain processing carried out on the basis of our legitimate interest is not appropriate.

- delete your Data: for example, and where applicable, if you no longer wish us to retain your Data.

You may further be entitled to object to the processing of your Data, based on grounds relating to your particular situation, or otherwise opt-out of the processing of your Data, where permitted under applicable laws (or opt-in if required). In this case, we will no longer process your Data unless we have compelling legitimate grounds to do so, such as when we need to establish, exercise or defend against legal claims.

In general, and particularly where required to do so under applicable laws, Park Place Technologies aims to respond to these requests within 1 month from receipt (extendable to a further 2 months in cases of particular complexity). If applicable under those laws, we will confirm receipt of your request within 10 days. Where entitled to do so, you may exercise any of the rights listed above by sending a written request to: dataprivacy@parkplacetech.com.

As a data subject, the data protection laws applicable to you may also entitle you to file a complaint with the competent supervisory authority for the protection of personal data, if you believe that the processing of your Data carried out by us is unlawful.

We adhere to the EU-U.S. Data Privacy Framework and UK Extension ("DPF") and commit to comply with DPF Principles. See https://www.dataprivacyframework.gov/. Under the DPF, we may be subject to U.S. authorized 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.

8) Amendments

This version of the Visitor Information Notice entered into force on the date displayed in its footer. We reserve the right to partly or fully amend this Information Notice, or simply to update its content, for example, as a result of changes in applicable law. In the event of substantial changes to the Information Notice, the updated text will be made available at the entrance of our premises and on our website.

Definitions

Personal Data: any information that makes a natural person identified or identifiable. For example, IP Address, email address (if it contains the details of a natural person), images depicting a person, are considered as Personal Data.

Sensitive Data: shall mean Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sex life or sexual orientation, including data relating to criminal convictions and offences or related security measures, or other types of Personal Data qualified as sensitive under applicable data protection laws, such as, where applicable, social security numbers, driver's license details, passport numbers, bank/financial account details, geolocation, or communications data (i.e., e-mail or regular mail contents).