General Data Privacy Policy AND Information Security Policy

Purpose

The purpose of this policy is to ensure compliance of all the business activities in PICO with the applicable privacy laws, data protection, and information security laws, such as the Israeli Privacy Law, the General Data Protection Rules of European Union and the California Consumer Privacy Act.

This policy outlines the handling practices of PICO and internal procedures regarding Personal Data (as defined below) and information security standard at PICO as a measure to protect the confidentiality, integrity and availability of any sensitive information owned, licensed, controlled, transmitted or processed by PICO.

Clients, employees, contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we engage with, collaborate with or acts on our behalf and may need occasional access to data.

We will update this policy when our information handling practices change.

Scope

PICO collects this information in a transparent way and only with the full cooperation and knowledge of the interested parties. Once this information is available to us, the following rules apply.

The policy shall be applicable for all the business activities of PICO. It has to be followed by all PICO's employees as well as by PICO's management.

Definitions

The following definitions are used to describe the General Data Privacy Policy:

Term	Definition
Personal Data	Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller/processor;
Consent	Freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data.

Verifications of Security, Privacy, and Compliance Controls

Our customers and regulations expect verifications of security, privacy, and compliance controls.

In PICO, we conduct internal verifications and controlled, performed from time to time by our CTO, Privacy Officer, and relevant management. PICO may also perform from time to time independent third party audits to provide this assurance.

Collected Data and Purpose of Processing

Accesses to our platform are logged for the purpose of security analysis reports and to defend against cyber-attacks. With the exception of the IP address, no personal data is ever collected or used in this connection. IP addresses are analyzed only in the event of a cyber-attack. Log data is promptly deleted or overwritten on a regular basis except the logs required by law.

In addition, following engagement with a client and during any activations made for our clients, and on behalf of our clients' only, we collect personal data (e.g., names, addresses, telephone numbers, or e-mail addresses) of our client's end users in connection with the operation of activations, only when our clients assure us, as a controller with respect to such collection of personal data, that their end users have voluntarily provided such data or provided the legal consent required, for us (e.g., through registration, contact inquiries, surveys, etc.) to collect, and that we are entitled to process or use such data by virtue of permission granted by our client or on the basis of a statutory provision.

As a general rule, we use such data only for the purpose for which our clients divulged the data to us, such as to answer inquiries, process orders or service requests, or grant access to certain information or offerings.

Sharing of Data

In connection with the operation of our platform and the services provided by way of the platform, PICO works with service providers such as hosting or IT maintenance service providers, for example.

These recipients may be located either in the US, Israel, the European Economic Area, or in countries outside of the European Economic Area, in which applicable laws offer a level of data privacy protection deemed as “adequate” by the European Union. In each case, PICO takes measures to ensure an appropriate level of data privacy protection and information security are taken internally within our group. For example, we share personal data with PICO subsidiary in the US, and ensure our US subsidiary implemented our Binding Corporate Rules for the protection of personal data.

Data is shared only in connection with and in compliance with applicable laws and regulations. We do not sell or otherwise market personal data to third parties.

Applicants and Employees Data Privacy Policy

The handling of privacy data coming from PICO’s employees or applicants for positions in PICO is detailed in internal policy **Human Resources Data Privacy Policy**.

Business Partners Data Privacy Policy

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data’s owner (exempting legitimate requests from law enforcement authorities)

Information Security

01	Throughout its lifecycle, all Personal Data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Data Protection Officer, given the level of sensitivity, value and criticality that the Personal Data has to PICO.
02	Any information system that stores, processes or transmits Personal Data shall be secured in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Data Protection Officer, given the level of sensitivity, value and criticality that the Personal Data has to PICO.
03	Individuals who are authorized to access Personal Data shall adhere to the appropriate roles and responsibilities, as defined by the Data Protection Officer with respect to each individual in PICO.

Enforcement

Violations of this Policy may result in suspension or loss of the violator's access and use privileges, with respect to Personal Data and PICO’s information systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with PICO. Civil, criminal and equitable remedies may apply.

Exceptions

Exceptions to this Policy must be approved by the Data Protection Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Data Privacy Contact

PICO provides support with any data privacy related questions, comments, concerns or complaints or in case an applicant, employee or business partner contact wish to exercise any of its data privacy related rights as mentioned in the section above.

The responsible Data Protection Officer of PICO is Aviv Paz and he can be contacted at aviv.paz@picogp.com.

Any complaints related to data privacy as well as any request for clarifications of the topics related to data privacy can be raised by mail at gdpr@picogp.com.

PICO will always use the best efforts to address and settle any requests or complaints brought to its attention. In addition, there is always the possibility to approach the competent data protection authority with requests or complaints.