

KIO DATA CENTERS PRIVACY NOTICE

- 1. IDENTITY AND REGISTERED ADDRESS OF THE DATA CONTROLLER.** METRO NET HOSTING, S. DE R.L. DE C.V. AND POWERHOST SOLUTIONS, S.A. DE C.V., (hereinafter referred to jointly or individually as "KIO DATA CENTERS"), with its registered address at Prolongación Paseo de la Reforma No. 5287, Cuajimalpa, Zip Code 05000, Mexico City, is responsible for the processing of your personal data, as well as for its use, protection, and confidentiality, in accordance with the Federal Law on Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), its Regulations, and other applicable legal provisions.

The data controller shall be the entity with which the data subject maintains, intends to maintain, or has maintained an employment, commercial, contractual, service-related, or other type of relationship. Where both companies jointly determine the purposes and means of the processing, they shall act as joint controllers and shall handle data subject requests through the same privacy contact channel.

For any matter related to this Privacy Notice, you may contact our Privacy Officer or Privacy Department at protecciondedatos_dc@kio.tech.

2. SCOPE AND INTENDED AUDIENCE.

This Privacy Notice applies to job candidates, current and former personnel, customers, prospective customers, representatives, authorized users, suppliers, contractors, visitors, event participants, and users of KIO DATA CENTERS' websites, portals, applications, or digital channels. The applicable purposes and categories of personal data will depend on the specific relationship each data subject has with KIO DATA CENTERS.

3. PERSONAL DATA COLLECTED.

To carry out the purposes described in this Privacy Notice, KIO DATA CENTERS may collect and process the following categories of personal data:

- **Identification and contact data:** Full name, address, telephone numbers, e-mail address, official identification, CURP (Unique Population Registry Code), RFC (Federal Taxpayer Registry Number), signature, image, or photograph.
- **Employment and academic data:** Résumé/Curriculum Vitae, employment and personal references, educational background, academic records, certifications, and professional experience.
- **Financial and asset-related data:** Tax information, bank account information (CLABE, SWIFT, or equivalent information), financial statements, and any other information necessary for contracting or complying with commercial obligations.
- **Browsing data (website visitors):** IP address, country, city, operating system, browser information, and information collected through cookies, web beacons, and similar technologies.

- **Corporate and representation data:** job title, company, authority and powers of representation, signature, professional contact information, and documentation evidencing such representation.
- **Technology and browsing data (website visitors):** IP address, device or session identifiers, access logs, country or approximate location, browser, operating system, language, date and time of access, pages viewed, time spent on the website, and data collected through cookies, web beacons, or similar technologies.
- **Access, security, and video surveillance data:** entry and exit records, access credentials, vehicle license plate numbers, and images and recordings obtained through closed-circuit television systems.
- **Sensitive personal data:** To the extent strictly necessary, KIO DATA CENTERS may process fingerprints or other biometric data used for access control or personnel authentication. Likewise, where necessary to protect the health, safety, or integrity of individuals, comply with legal obligations, address public health emergencies, implement risk prevention measures, or ensure the continuity of KIO DATA CENTERS operations, KIO DATA CENTERS may process information relating to health conditions, travel history, contacts potentially exposed to health-related risks, or any other information strictly necessary for such purposes. Such processing shall be carried out under strict confidentiality measures and only for the period necessary to fulfill the purposes that justify it.

KIO DATA CENTERS undertakes that sensitive personal data shall be processed under the strictest physical, technical, and administrative security measures and solely for the legitimate, specific, and necessary purposes described in this Privacy Notice.

4. PURPOSES OF PROCESSING. Primary Purposes. (Necessary for the establishment, maintenance, and performance of the legal relationship with KIO DATA CENTERS):

- **Applicants and Employees:** Candidate evaluation and recruitment processes, background verification, creation and maintenance of personnel records, registration procedures with the Mexican Social Security Institute (IMSS), payroll administration, provision of work tools and equipment, and administration of applicable insurance benefits.
- **Clients and Prospective Clients:** Provision of services, technical support, invoicing, collection activities, handling of complaints and claims, and registration within accounting and administrative systems.
- **Suppliers:** Procurement management, reference verification, payment processing through bank transfers, and maintenance of contractual records.
- **Visitors and Event Participants:** Access control to physical and virtual facilities, security-related video surveillance (images are retained for up to ninety (90) days), and the distribution of event agendas and confirmations.

Images obtained through video surveillance systems shall be used exclusively for security purposes, access control, and the protection of individuals and property, and may be

retained for up to ninety (90) calendar days, unless a different retention period is required by applicable law.

Secondary Purposes. (Not necessary for the legal relationship but intended to provide a better experience and service)

- Distribution of newsletters, promotional materials, offers, advertising, marketing activities, and commercial prospecting.
- Conducting satisfaction surveys, quality assessments, statistical studies, and trend analyses.
- Use of photographs, interviews, testimonials, or references for corporate communications, institutional publications, and social media.

If you do not wish your personal data to be processed for any or all of the secondary purposes described above, you may express your refusal within five (5) business days following the collection of your personal data by submitting a request to protecciondedatos_dc@kio.tech.

Your refusal to allow the processing of your personal data for secondary purposes shall not be grounds for denying the products or services requested, nor shall it affect the legal relationship you maintain with KIO DATA CENTERS.

5. TRANSFERS AND DISCLOSURES OF PERSONAL DATA.

KIO DATA CENTERS may transfer your personal data without requiring your consent in the cases permitted under applicable law, including those provided for in Article 37 of the Federal Law on Protection of Personal Data Held by Private Parties, such as transfers to parent companies, subsidiaries, affiliates within the same corporate group, competent authorities, financial institutions, insurance companies, or third parties where such transfers are necessary for the maintenance, performance, or execution of a legal relationship with the data subject, or where required by law.

Likewise, KIO DATA CENTERS may disclose your personal data to service providers acting as data processors, including cloud storage providers, hosting providers, technology support providers, human resources administration providers, payment processing providers, data analytics providers, and other service providers related to KIO DATA CENTERS operations. Such data processors shall process personal data solely in accordance with KIO DATA CENTER instructions and for the purposes established in this Privacy Notice.

Due to the nature of KIO DATA CENTERS operations and the use of technological platforms, storage services, information processing services, digital infrastructure, or corporate services provided by third parties, certain personal data may be processed, stored, or backed up on servers located within or outside the United Mexican States. In such cases,

KIO DATA CENTERS shall adopt the contractual, organizational, and security measures reasonably necessary to ensure that recipients and data processors maintain adequate levels of protection and confidentiality in accordance with applicable law and KIO DATA CENTERS internal policies.

In all cases, KIO DATA CENTERS shall implement contractual, administrative, and security measures reasonably necessary to ensure that third parties and data processors involved in the processing of personal data comply with applicable legal requirements and protect such information in accordance with the principles and obligations established under applicable regulations.

6. ARCO RIGHTS AND WITHDRAWAL OF CONSENT.

You have the right to:

- Obtain information regarding the personal data we hold about you and the purposes for which it is processed (Access).
- Request the correction of inaccurate or incomplete information (Rectification).
- Request the deletion of your personal data when you believe it is not being processed in accordance with applicable law (Cancellation).
- Object to the processing of your personal data for specific purposes (Opposition).
- Withdraw any consent previously granted for the processing of your personal data where legally permissible.

To exercise any of these rights, you must submit a request to the Privacy Department via protecciondedatos_dc@kio.tech, including:

1. Full name of the data subject.
2. Address or e-mail address for notifications.
3. Copy of a valid official identification document or evidence of legal representation.
4. Clear and precise description of the personal data with respect to which the right is to be exercised.
5. Any information facilitating the location of the relevant personal data.

KIO DATA CENTERS shall communicate its determination within a maximum period of twenty (20) business days following receipt of the request.

If the request is granted, it shall be implemented within fifteen (15) business days following notification of the corresponding determination.

To withdraw your consent, you must follow the same procedure established for exercising ARCO Rights.

7. LIMITATION OF USE OR DISCLOSURE OF PERSONAL DATA.

If you wish to limit the use or disclosure of your personal data for promotional or advertising purposes, you may submit a request to protecciondedatos_dc@kio.tech.

Likewise, where applicable, you may register with the Public Registry to Avoid Advertising (REPEP), administered by the Federal Consumer Protection Agency (PROFECO).

8. COOKIES AND TRACKING TECHNOLOGIES. Our websites use cookies, web beacons, and similar technologies to:

- Identify user sessions.
- Remember browsing preferences.
- Analyze website traffic and usage.
- Improve the browsing experience.
- Obtain usage and performance statistics.

Through these technologies, we may collect information such as IP address, approximate location, browser type, operating system, language preferences, access date and time, pages visited, and duration of visits.

You may configure your browser to reject or delete cookies; however, certain website functionalities may be limited or affected.

9. DATA RETENTION AND SECURE DISPOSAL.

Personal data will be retained for as long as necessary to fulfill the purposes communicated in this Privacy Notice, maintain the relevant relationship, and comply with applicable limitation periods, legal obligations, audits, investigations, or the establishment, exercise, or defense of legal claims. Once the applicable retention periods have expired, the personal data will be deleted, destroyed, anonymized, or blocked in accordance with KIO DATA CENTERS' internal procedures and applicable law.

Video surveillance recordings will ordinarily be retained for up to 90 calendar days, unless they must be preserved for a longer period in connection with an incident, investigation, request from a competent authority, legal or administrative proceeding, or a different statutory retention period. Personal data relating to unsuccessful job candidates will be retained only for the period authorized or necessary for consideration in connection with future vacancies and may be deleted earlier at the data subject's request, unless a legal obligation requires its continued retention.

10. CONSENT.

Where consent is required, KIO DATA CENTERS will obtain it before processing through mechanisms that allow the data subject's wishes to be demonstrated. Consent will be

express where financial or asset-related personal data are processed in circumstances in which such consent is legally required, and express and in writing where sensitive personal data are processed, except where an applicable legal exception applies.

Making this Privacy Notice available does not replace any specific consent required for the processing of sensitive personal data, transfers subject to consent, secondary purposes, use of a person's image, or non-essential tracking technologies. KIO DATA CENTERS will retain evidence of the consents obtained and will allow data subjects to withdraw their consent in accordance with applicable law.

11. SECURITY MEASURES AND COMPETENT AUTHORITY. KIO DATA CENTERS implements administrative, technical, and physical security measures reasonably necessary to protect your personal data against damage, loss, alteration, destruction, or unauthorized access, use, or processing.

Should a security breach occur that significantly affects your economic or moral rights, KIO DATA CENTER shall promptly notify you through the available contact channels.

If you believe that your right to the protection of personal data has been violated by any act attributable to KIO DATA CENTER, or if you believe that the processing of your personal data violates applicable legal provisions, you may file a complaint before the competent authority responsible for personal data protection, or any authority that may legally replace it, in accordance with the procedures established under applicable law.

12. VIDEO MONITORING AND PHYSICAL ACCESS CONTROL. KIO DATA CENTERS' facilities may be equipped with video surveillance systems and access controls. Visible short-form privacy notices will be displayed before individuals enter monitored areas. Images, recordings, and access records will be used for security, access control, the protection of persons and property, incident investigation, and compliance with applicable obligations. They will not be used for incompatible purposes without prior notice and, where applicable, the corresponding consent.

13. AMENDMENTS TO THIS PRIVACY NOTICE.

KIO DATA CENTERS reserves the right to amend or update this Privacy Notice at any time as a result of legislative or regulatory changes, internal policies, new service requirements, or privacy practices.

Any amendments shall be made available through <https://kiodatacenters.com/es-mx/>

Where an amendment introduces new purposes, transfers subject to consent, or other changes requiring renewed authorization, KIO DATA CENTERS will provide notice through an appropriate means and obtain the corresponding consent before commencing the new processing activity.

Last Updated: July 2026.